2019 CTIC
网络安全分析与情报大会
CYBER THREAT INTELLIGENCE CONFERENCE

第三方供应商信息安全风险管理实践

陈建
平安集团首席安全官

背景问题
Back Ground

01 与企业合作的供应商有能力保护相关隐私安全吗?

2016年Gartner报告<The State of Digtital Third-Party Risk 2016 Report>指出:59%的信息泄露是由于第三方供应商导致的，全球财富500强中75%的企业将供应商风险提升至董事会层面。

2018年波耐蒙研究所(Ponemon Institute)研究指出：在英国和美国约有60%的公司表示他们通过第三方遭受了数据泄露，且其中只有35%的企业认为自己有行之有效的第三方风险管理计划。

02 董事与高管在网络安全监督方面责任/难度越来越大

每当出现高度曝光的数据泄露事件时，往往伴随的是相应上市企业股价的断崖式下跌及重大声誉危机，如今管理网络风险已成为企业董事和高管最大监督挑战之一，甚至已经成为他们的个人风险。

为了更好的理解企业安全风险现状，董事会在不断的要求增加安全高管的汇报频度，但在Bay Dynamics 的一项覆盖125位活跃董事会高管调查结论指出，81%的受访安全高管认为频繁的安全汇报分散了大量工作精力，71%的董事会成员认为安全风险汇报过于技术化，难以理解。

美国零售巨头TARGET

黑客通过其空调供应商HVAC的远程维护系统入侵到TARGET的内部网络，导致近1亿用户数据泄露

电动汽车独角兽特斯拉

黑客入侵了其工业自动化供应商level one的数据库，导致近157GB的蓝图、工厂原理图、客户资料（合同、发票、工作计划等）泄露

CASE

供应链信息安全问题再次增加了信息安全治理的广度和难度

国内智能手机制造商

黑客通过入侵其物流供应商系统窃取相关数十万用户订单数据

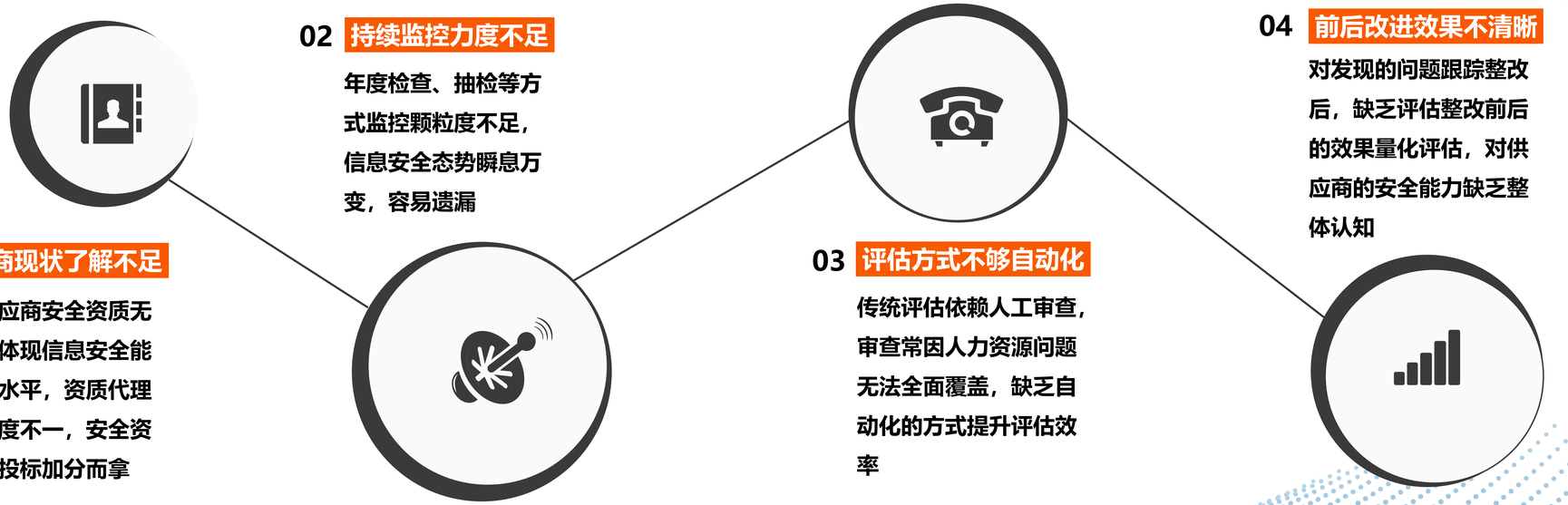
国内金融保险企业

因其供应商**健康科技的网站存在漏洞，泄露数十万条保险用户的险种、手机号、身份证号、密码信息

供应商风险评估的普遍缺位

		业务收益	业务风险
		引入供应商需要平衡业务收益与潜在风险，但往往风险评估是缺位或不详尽的	
BPO	电话客服 制卡 物流 商旅 代发工资	提升非核心业务能力效率 企业资源聚焦核心业务	安全声誉风险、安全合规风险、人员操作风险
营销获客	营销短信 CPS、CPA广告 电话销售	提升业务运营指标	数据隐私泄露、滥用风险 安全声誉风险
ITO	外包软件开发 机房托管 IT运维托管	借助第三方在技术领域能力 知识快速满足业务需求	技术安全质量风险 人员操作风险

供应商风险评估的现状与挑战



01 供应商现状了解不足

仅凭供应商安全资质无法正确体现信息安全能力真实水平，资质代理严谨程度不一，安全资质仅为投标加分而拿

02 持续监控力度不足

年度检查、抽检等方式监控颗粒度不足，信息安全态势瞬息万变，容易遗漏

03 评估方式不够自动化

传统评估依赖人工审查，审查常因人力资源问题无法全面覆盖，缺乏自动化的方式提升评估效率

04 前后改进效果不清晰

对发现的问题跟踪整改后，缺乏评估整改前后的效果量化评估，对供应商的安全能力缺乏整体认知

平安供应商风险评估平台

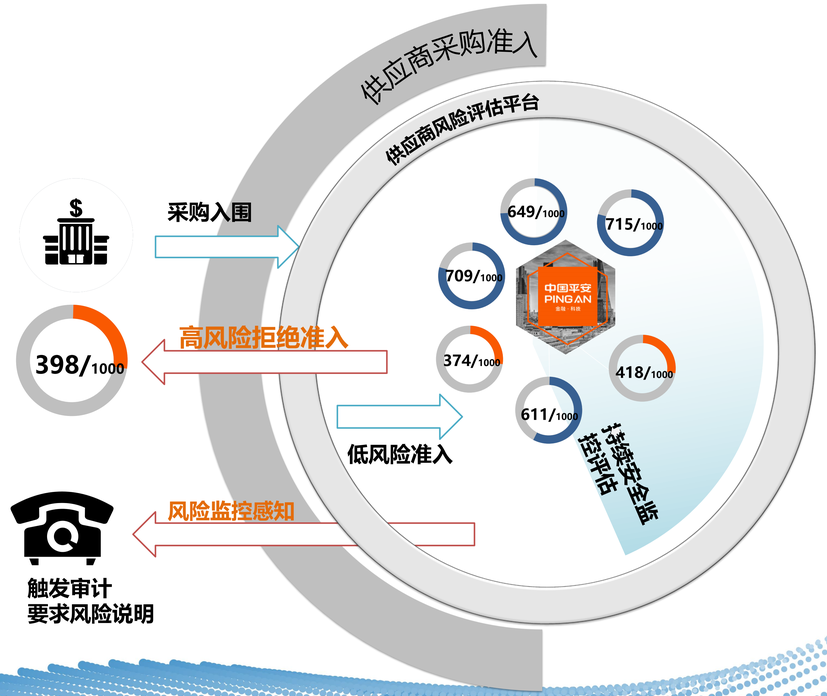
在供应商入围阶段启动信息安全评估

- 通过平台自动化对供应商进行安全评估
  1-2周内拿到评估结果和报告

- 对发现高风险的供应商要求进行风险说明或拒绝合作

对合作供应商信息安全的持续监控

- 对已合作供应商的持续安全态势监控，一旦发现新增风险，向业务合作方披露风险并触发下一步的安全审计要求进行风险说明



平安供应商风险评估平台

自动化收集的企业信息安全情报

实时采集分析

信息安全负面舆情

企业数据泄露、黑客攻击、严重漏洞、员工渎职新闻事件负面舆情

风险事件 incidents

威胁情报与缺陷扫描

与信息资产关联的威胁情报，来自公开、商业、威胁情报联盟的情报信息

网络空间测绘

网络空间内公开可发现的信息资产信息采集整理，对相关资产缺陷进行扫描监控

缺陷扫描 evaluation

每日更新的企业安全评分

SRS security rating services
信息安全量化服务

自动化收集企业信息安全水平相关信息，通过安全大数据对企业信息安全水平进行量化评价

通过在线问卷收集的安全控制信息

问卷评估 questionnaire

安全控制评估问卷

端到端的供应商内部安全控制评估问卷，基于等保、ISO27001、行业监管框架设计

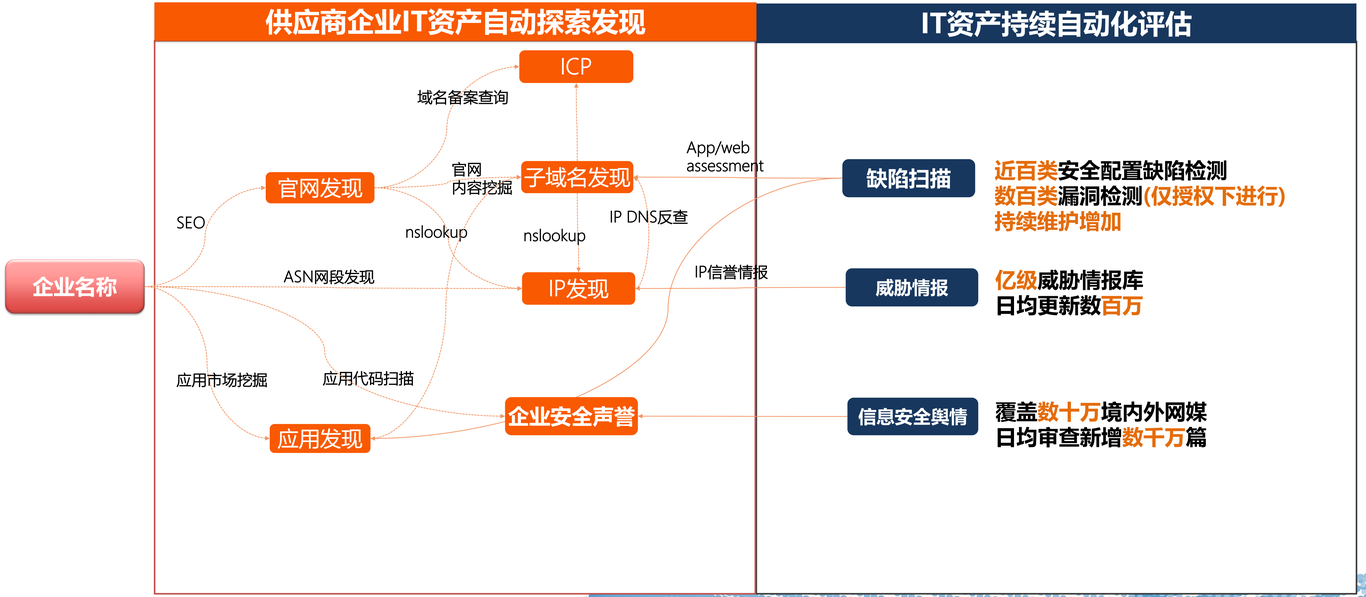
企业基本信息

企业基本工商注册信息(自动化)
企业上下游关联公司关系
企业信息安全资质

安全资质 certification

平均 周内即可完成的问卷

供应商资产图谱的自动探索与评估



供应商安全控制能力的自动化问卷审查

采购、业务、信息安全

通过供应商风险评估平台的行业评估问卷模板筛选与供应商企业匹配的安全评估问卷

安全几何信息安全法律规范知识库

国际法规	地区法规	行业监管法规
《ISO/IEC 27001：2013 信息技术 安全 《ISO/IEC 27000：2016 信息技术 安全 《ISO 22301：2012 公共安全	内地：《国家网络安全事件应 《信息安全等级保护管理 《中华人民共和国网络安全法》 香港：《监管政策手册-TM-G-2-... 《降低及紓減與互聯網交易	金融：《非银行支付机构信息科技 《银行业金融机构重要信 保险：《保险机构内部审计工 《保险公司信息系统安全管 证券：《证券期货业信息安全事 《证券公司集中交易安全

PII(个人隐私)	《个人信息去标识化指南》《电信和互联网用户个人信息保护规定》《个人资料(私隐)条例》...
云计算	《CSA云计算安全技术要求-PaaS安 《CSA云计算安全技术要求-SaaS 《CSA云计算安全技术要求-Ia

100+ 安全相关法规

600+ 安全评估问题

新法规持续解读 录入

集团安全管理

BPO企业模板

精准营销企业模板

电子问卷以邮件发送给供应商企业回答

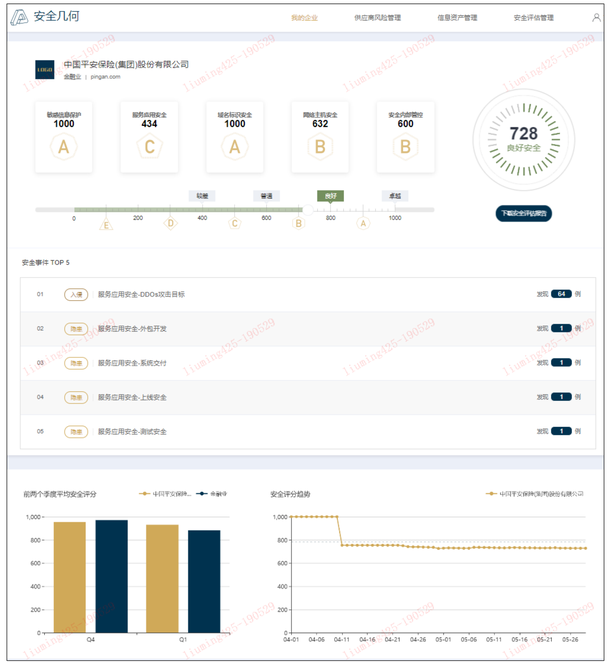
平均两周内完成问卷

问卷答复结果反馈计入评分

01

安全评估概览

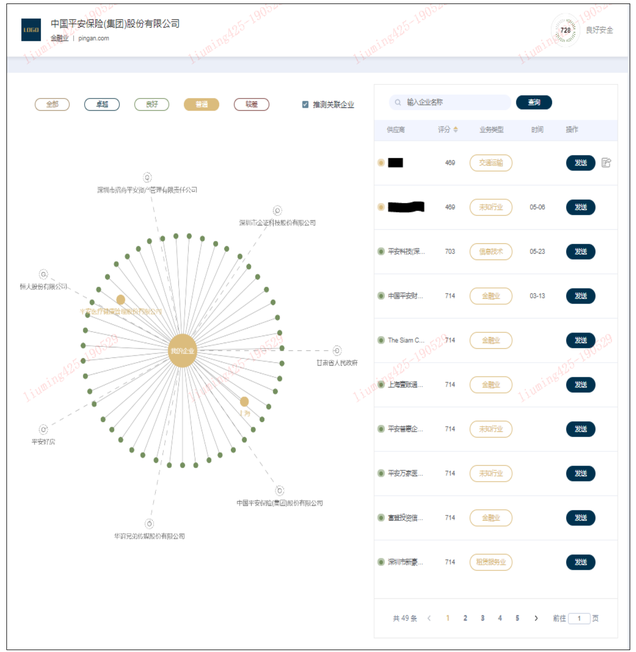
展示自身企业的安全评分与趋势，影响评分评级的目前首要问题



02

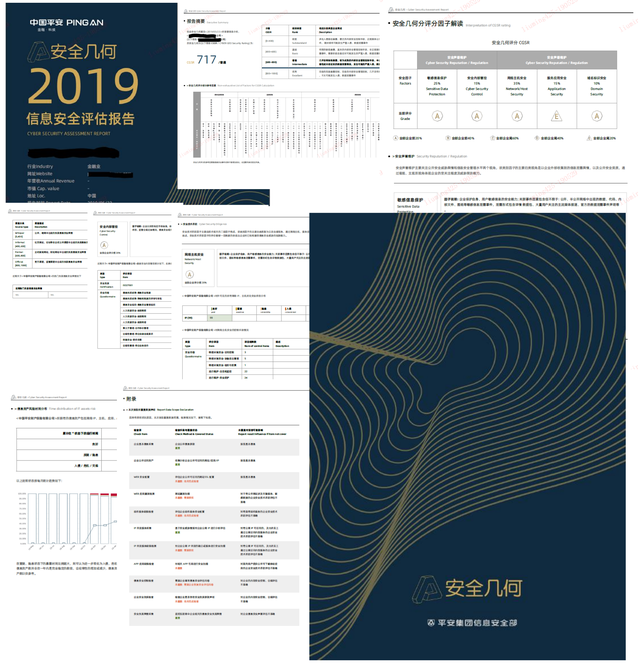
供应商风险管理

展示录入合作供应商，并展示合作供应商目前的风险态势



03 自动化生产安全报告

展示录入合作供应商，并展示合作供应商目前的风险态势



供应商风险评估平台整体方向

- 自有威胁情报
- 威胁情报联盟
- 商采开源威胁情报

威胁情报

- 网络空间资产发现与描述
- 资产属主自动化发现维护

网络空间测绘

合规知识库

- 行业、地区安全法规
- 法规控制项、控制问题、控制框架

安全几何

自动化缺陷审计

- 资产安全配置缺陷、漏洞自动化审计
- 缺陷、漏洞与合规检查项的关联关系

- 自动化生成的安全评分详细阐述报告，帮助进行安全汇报与确定安全投资决策

安全研判报告

安全评分评级

- 标准化安全评分评级，在同行间横向比较自身水平

平安合作方安全体检

采购准入　投资并购

供应商风险管理平台

在线审计　现场审计

THANK YOU

CTIC