互金威胁与安全建设

田国华　时间：2017.6　上海

田国华

资深信息安全经理/上海拍拍贷

- 专注信息安全12年；
- 前携程高级网络安全经理；
- 现上海拍拍贷任职；
- CISSP、CISA、PMP、ITIL 、CCNP等认证证书；
- 10余项技术发明专利；
- (ISC)² 上海分会理事；

CISA Certified Information Systems Auditor An ISACA Certification

PMI Project Management Institute PMP® Certified

CISCO CCNP

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP®

(ISC)² CHAPTER SHANGHAI

ITIL® FOUNDATION

目录

01

互金威胁

|互联网&金融行业状况

拍拍贷 ppdai.com

6.95亿

手机网民

截止2016.12

占比95.1 连续三年超10%增速

7.31亿

中国网民总数

截止2016.12

普及率达53.2%

20%

12万亿

截止2015.12

互金交易规模12万亿，接近GDP20%

互金用户

截止2015.12

世界第一

5亿

|安全生态在恶化

PC端新增恶意程序**1.9亿**

497多万台用户电脑遭到了敲诈者病毒攻击

Android新增恶意程序**1403.3万**个，新增手机勒索软件**17万**，170台手机遭到攻击。

新增钓鱼网站**196.9万**个，共拦截钓鱼攻击**279.5亿**次，网站被黑而搭建的钓鱼网站为19.0%

网络诈骗举报**20623**例，举报总金额**1.95亿**余元，人均损失**9471**元

金融理财是涉案金额最高的诈骗形式

|互金主要安全风险

数据泄露威胁

在全球范围内，2016年上半年已曝光的数据泄漏事件高达974起，数据泄漏记录总数超过了5.54亿条；

2017年3月，公安部破获同盗卖公民信息的特大案子，**查获涉及物流、医疗、社交、银行等各类被盗公民个人信息达50亿条**，主要罪犯郑某鹏于2016年6月底**入职京东**，是尚处于试用期的网络工程师。

2016年10月，湖南一**银行支行行长**，却出售自己的查询账号给中间商,**售卖公民银行个人信息257万条**，涉及征信报告、账户明细、余额等个人敏感信息。

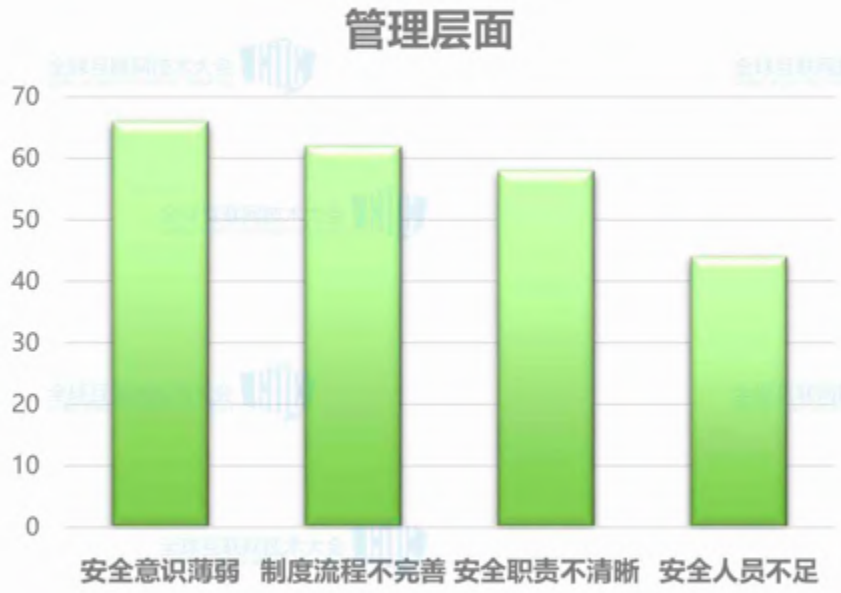
2016年9月23日，**雅虎宣布有至少5亿用户账户信息被黑客盗取**，盗取内容包括用户的姓名、电邮地址、电话号码、生日、密码等，甚至还包括加密或未加密的安全问题及答案。同时，**这也打破史上最大单一网站信息遭窃的纪录。**

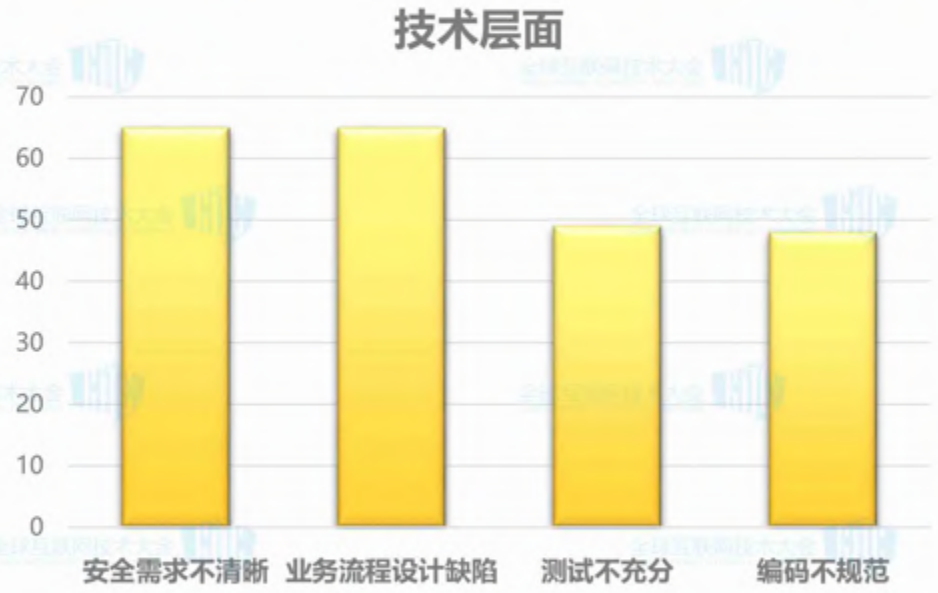
互联网金融安全漏洞

02

关注焦点

|安全问题产生的原因





|信息安全管控趋势分析

建立和完善信息安全管理体系将会变得越来越重要

随着互联网金融的深化发展，以体系化的思路管理信息安全将是一个必然的趋势。目前业务较成熟、规模较大的互联网金融企业都已经建立了信息安全管理体系，处于成长期的企业，随着业务规模的扩大，管理流程的复杂化，建立信息安全管理体系，从管理和技术两方面提升信息安全管控能力也会变的越来越迫切。

行业成熟度的提升将促进对安全投入的增加

40%认为企业信息安全投入不足。而随着互联网金融企业管理成熟度的提高，对信息安全增加投入也是一个必然的趋势。

从信息安全事件的关注程度层面来看，由于信息安全事件造成的社会舆论极大地影响到公众对企业的信任，所以互联网金融行业相较其他行业而言更加关注信息安全事件。

网络信息安全保障上升至国家层面

2016年12月27日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》，提出“推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。”

2015年4月23日，美国国防部发布了最新的网络空间安全战略，提出发展网络力量、加强网络防御、实现进攻型网络威慑。首次公开表示把网络战作为今后军事冲突的战术选项之一。并将中国、俄罗斯、伊朗、朝鲜共同列为最大的潜在威胁对象。

网安法带来的挑战

个人隐私保护

- 强调个人信息和隐私保护。
- 规范个人信息收集和使用。
- 企业的数据安全延展到影响范围更大的个人隐私信息。
- 明确处罚措施，包括停业、吊销执照和罚款等。

网络运营者

- 明确网络运营者定义和安全要求。
- 大部分金融机构将可能成为网络运营者。
- 等级保护是基本要求。
- 明确处罚措施，包括停业、吊销执照和罚款等。

关键信息基础设施

- 对关键信息基础设施提出更高安全要求。
- 尚未明确关键信息基础设施的范围。
- 明确处罚措施包括停业、吊销执照和罚款等。

个人信息与数据跨境

- 外资企业、跨国集团和具有海外业务的组织通常需要将数据传至国外。
- 敏感数据应存储在国内。
- 明确处罚措施，包括停业、吊销执照和罚款等。

03

规划思路

|Blue Lava 信息安全成熟度模型

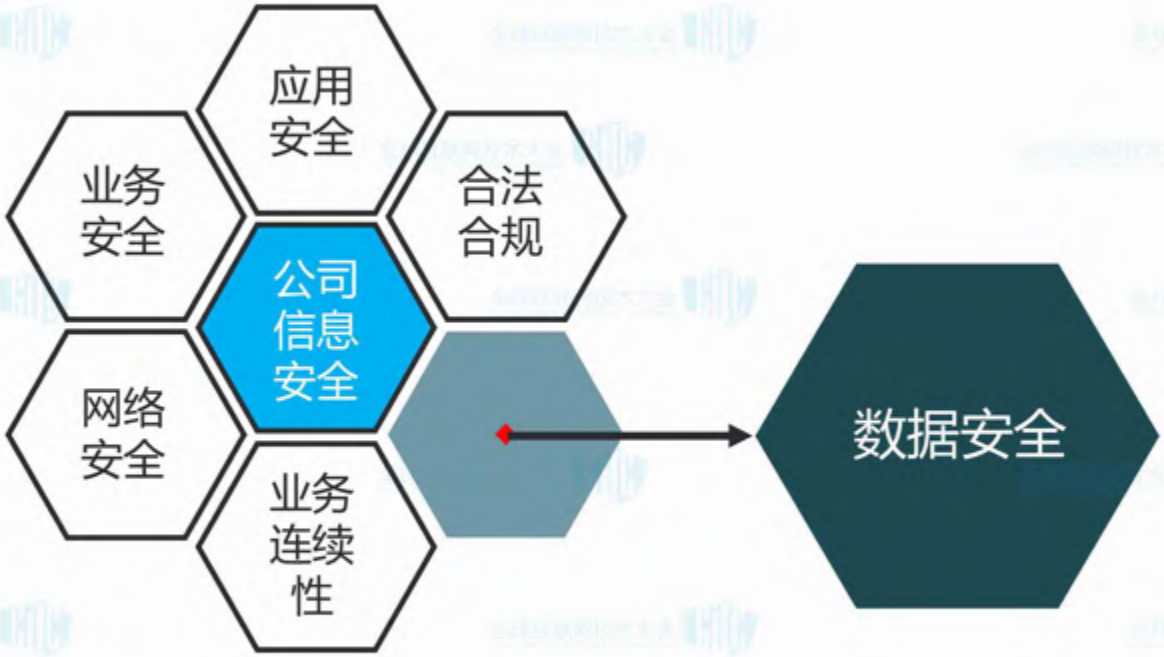
防御与处理	标准化驱动	基于风险评估的方法
•缺少威胁检测的手段，对安全现状不了解； •缺少统一的安全规划； •人员不足； •报告缺少数据支持； •高层领导支持不足； •资金支持不足； •忙于应急；	•基于标准化来驱动安全； •主动满足一些法律法规或行业标准来提升安全： -ISO 2700X -PCI DSS -行业监管要求 -公安部等保安全 -上市SOX 合规	•基于风险评估结论采取不同安全层级的纵深防护体系； •用户行为分析； •新技术的快速响应； •不同角度分析问题；


初创企业位置

一般上市公司的标准

业内最佳实践

|公司信息安全关注点



安全为业务创造价值

|信息安全规划目标

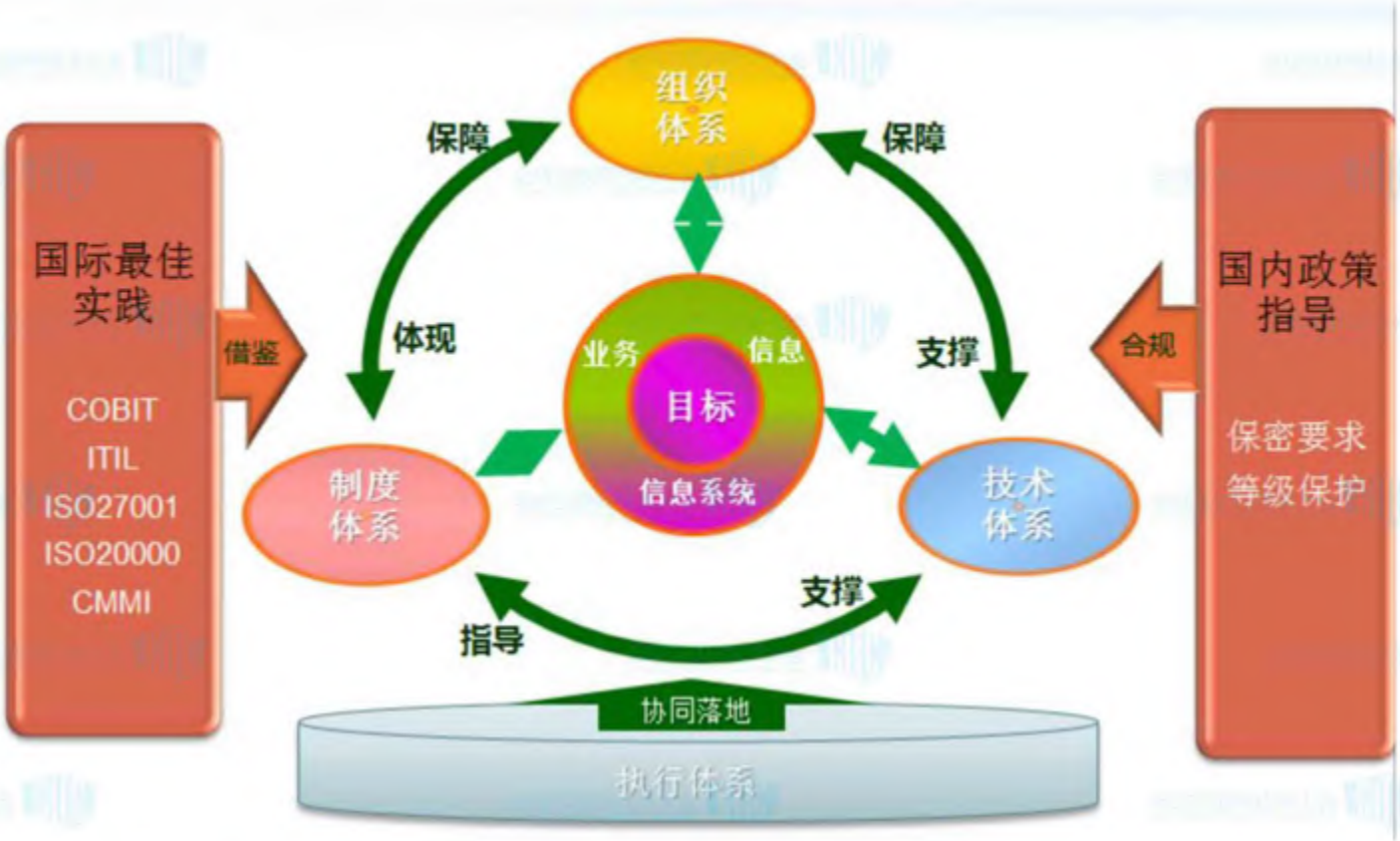
制定信息安全规划，以满足企业不断发展的业务要求和IT合规审计要求，保障包括借贷交易平台、手机APP在内的应用系统的安全、稳定运行。

信息安全规划

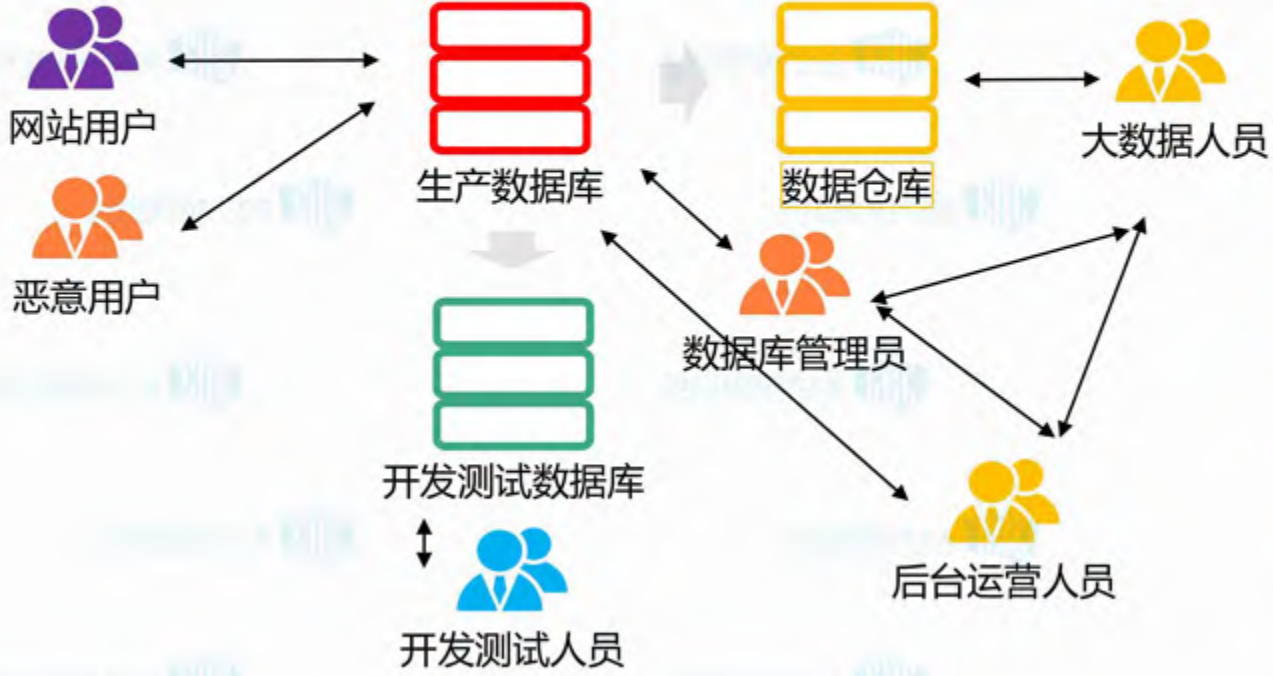
制定信息安全规划，以提高企业信息安全保障能力，完善信息安全技术防护体系及信息安全管理体系。

制定信息安全规划，以明确信息安全保障能力建设路线图，确保信息安全建设分阶段有序进行。

信息安全蓝图



数据安全防泄漏



主要防护措施

- Web安全防护
- 数据库加密
- 数据脱敏（透明）
- HDLP/NDLP
- 日志、流量审计

04

安全建设

|安全建设阶段

拍拍贷 ppdai.com

优先解决业务痛点
做一些基础的“保命”工作；

1
救火阶段

2
体系化建设

扎实安全基础建设
建立安全体系+少量自研工具
+商用解决方案

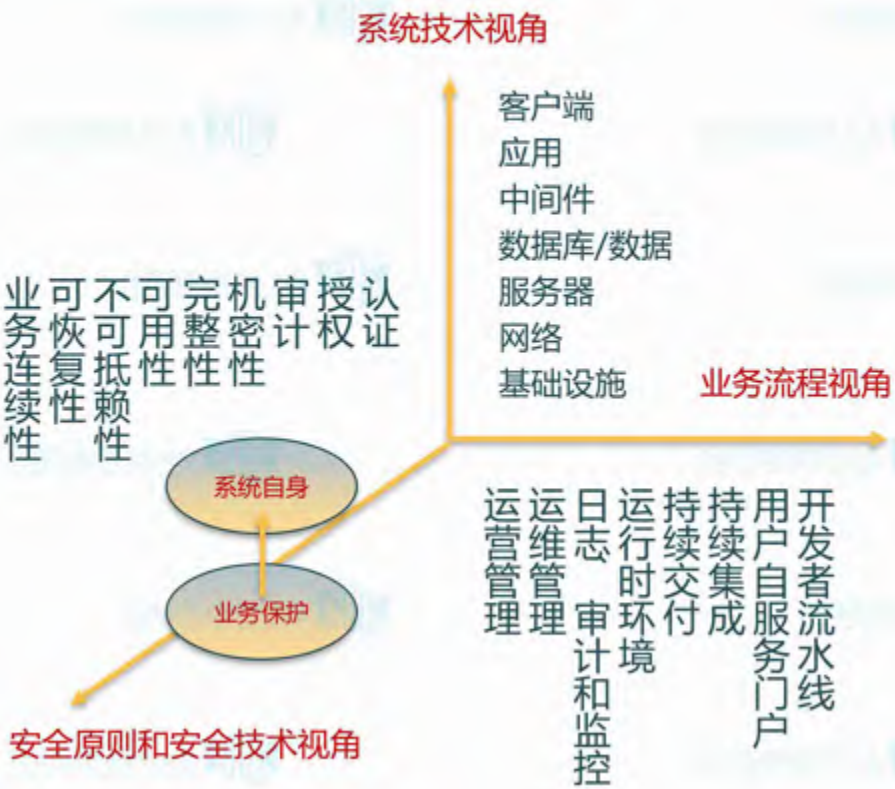
3
持续优化

自我研发和自动化
安全大数据
持续安全运营

4
高阶阶段

安全自适应、智能化
阻止、检测、响应、预测

|安全架构



|基本的安全理念依然重要

自适应安全架构


威胁联动
主动探索分析
预测攻击
基准化安全系统
加固和隔离系统
攻击防御
误导攻击者
攻击拦截
持续监控
和分析
系统修复
监测事故
设计更改
确认及定性危险
回溯分析
事故鉴定
处理事故
入侵检测

|信息安全成功的关键

- 安全策略、目标和活动应该反映业务目标
- 来自高级管理层的明确的支持和承诺
- 实施信息安全的方法应该与组织的文化保持一致

- 深刻理解安全需求、风险评估和风险管理
- 向所有管理者和员工有效地推广安全意识
- 建立完整而平衡地测量体系，用来评估信息安全管理体系的表现，提供改进的反馈建议


Thank you !
Q&A