

风险管理驱动下的主动安全变革

京东信息安全战略官
吉贻俊 (Neil Ji)

以安全保发展 以发展促安全 建久安之势 成长治之业



风起云涌

以正合 以奇胜

其命维新

盖有非常之功
必待非常之人

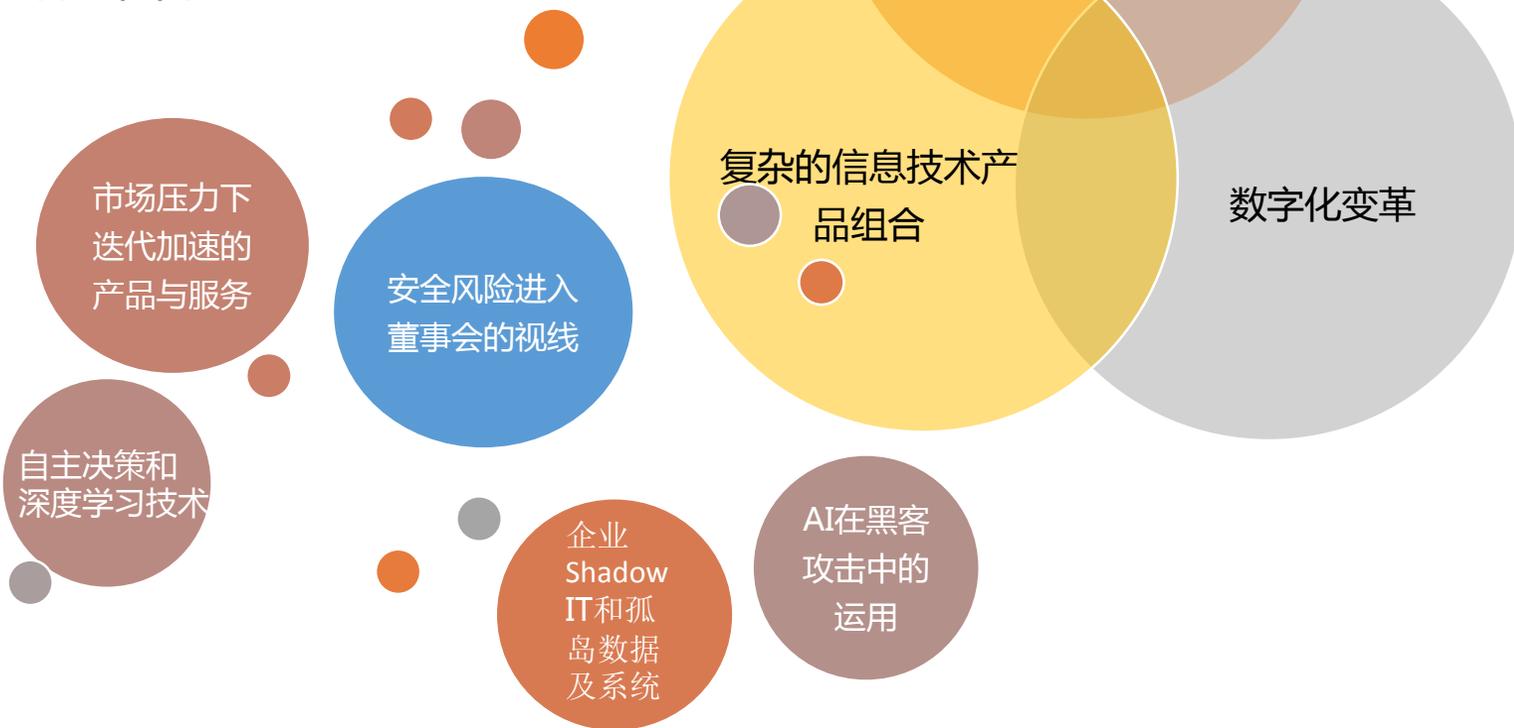
风起云涌

只在此山中
云深不知处



风起云涌

- 国际国内及行业内合规要求和监管不断升级
- IT正从支持业务效率型向业务创新业务驱动转型
- 企业内部信息技术纷杂数据汗牛充栋治理困难





千人千面



京东云 Cloud



互联网金融 Fintech



无界购物



无人超市

物流 Logistics



用户参与



无人车



个性化需求



无人仓

核心驱动
场景和数据



无人机



智慧供应链



2.5亿 活跃用户

15 PB / 天



智能家居 Smart Home



人工智能 AI



智能客服



大数据 Big Data



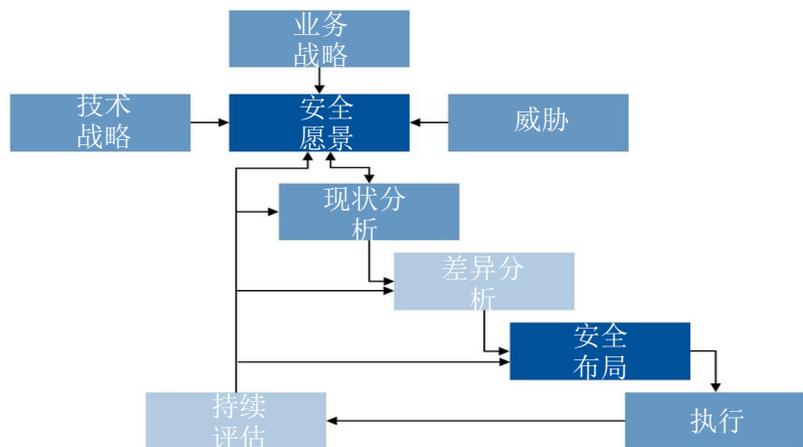
京东安全

以正合 以奇胜

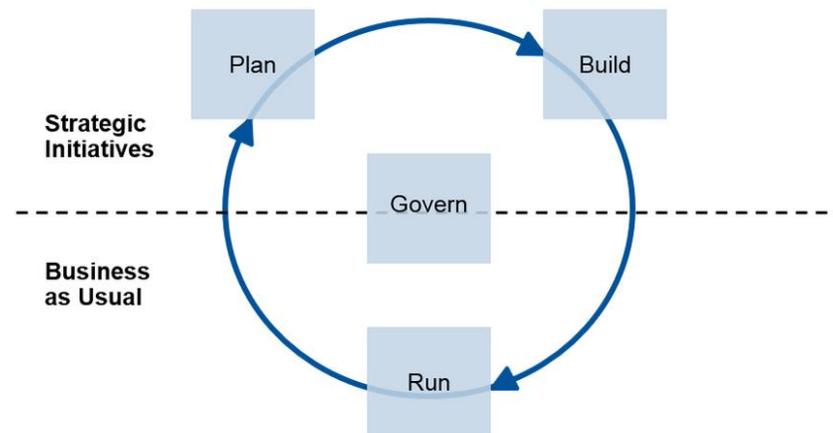
成年人学习的目的，应该是追求更好的思维模型，而不是更多的知识。
在一个落后的思维模型里，即使增加再多的信息量，也只是低水平的重复。

以正合，以奇胜

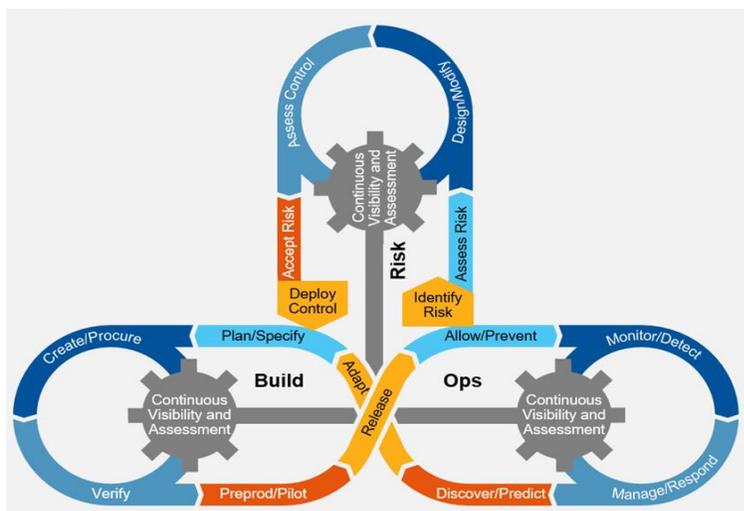
战略规划的起点与根本



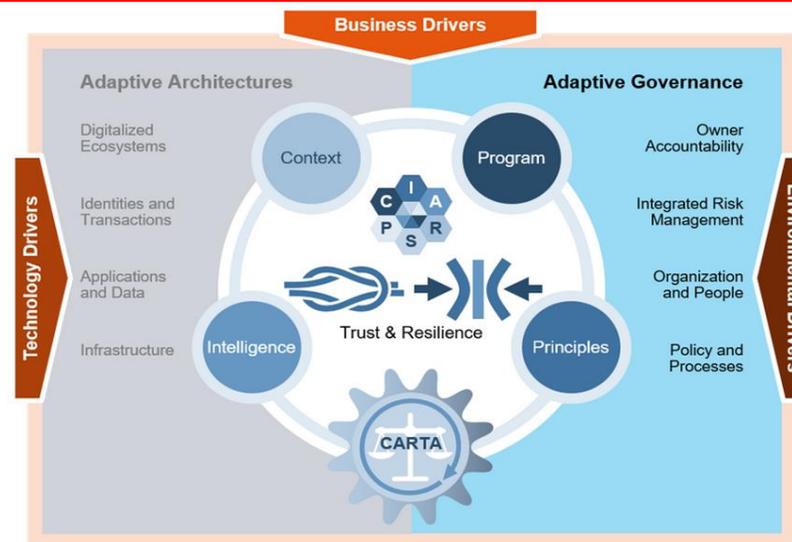
持续优化



融会贯通



互联网+下的安全愿景



Source: Gartner

以正合，以奇胜

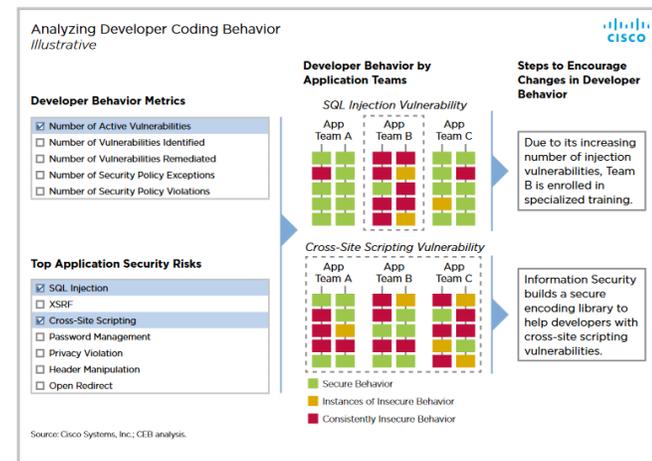
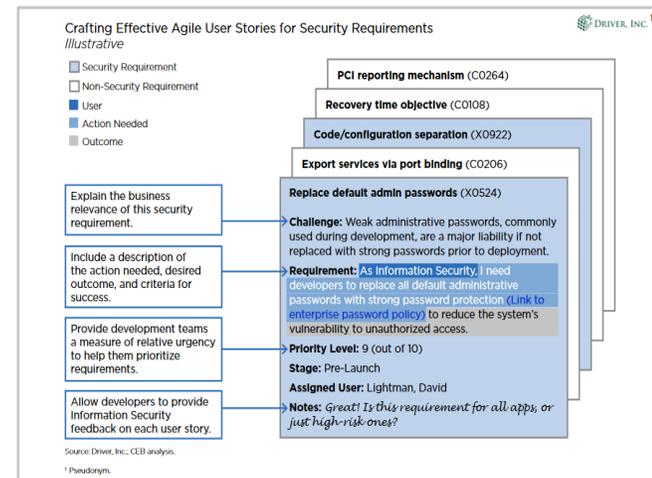
当下的数字化变革正向从改进企业运维效率到改变企业整体业务模式自我进化，但传统的信息安全治理体系和流程难以与当前产品服务开发速度匹配。

	以安全为导向	以业务为导向
职责	风险决定的促进者 信息安全团队帮助业务部门做出风险处置的决定	数字业务的赋能者 信息安全部门帮助企业实现数字化的变革
范围	垂直和横向的集成 信息安全部门向各产品线和业务部门提供及调整安全服务	垂直支持和横向集成 支持各产品线安全团队但继续承担企业层面的安全风险和战略挑战
架构	集中 CISO集中管理信息安全职能	聚合 产品团队将根据信息安全团队要求进行各自部分信息安全管理
活动	建议与实施 信息安全团队向权益相关方提供安全解决方案的建议，并实施选定的解决方案	建议与管理 信息安全团队向权益相关建议安全方案，并引权益相关方实施安全方案和运维。

奇 = 速度？人才？
技术？治理？...

在数字化引领企业业务转型的时代，信息安全怎样才能更高效的支持敏捷开发？

- 将安全治理嵌入到开发人员工作流程中
- 提供开发人员友好易懂的安全指导
- 开发人员责任制 (KPI)



其命维新

或者创新，或者消亡。



其命维新



- 斯坦福SAIL-京东建立联合AI实验室
- 联合研究项目-清华, UC Berkeley, Indiana University, and Iowa State University
- 研究领域: IoT安全, AI 安全, NLP, 威胁大数据



盖有非常之功，必待非常之人

大风起兮云飞扬，
安得猛士兮守四方



盖有非常之功，必待非常之人

信息安全团队目前的挑战不但来源于升级的技术也来源于永远有限的资源

- 能够向业务证明安全有效性的资金投入
- 能够在数字化时代应对复杂而职能变换的具有多样性技能的安全人才

增加雇佣新安全员工

*据Gartner 2017高管年展望会议报告中统计，企业聘用一位新安全员工的平均时间为130天。

提高目前员工的有效性和投入程度

*You're either on the bus or off the bus. — Ken Kesey

数字化和业务需求要求安全人员能适应更多样的专业职能

*新职能举例：

- ❑ 产品安全专家
- ❑ 销售和客户安全支持专家
- ❑ 应用安全专员
- ❑ 安全数据科学家
- ❑ 威胁对象分析专家
- ❑ 业务模型专家
- ❑ 业务安全咨询专家
- ❑ 安全推广大使
- ❑ 安全沟通专员等



“

Thank

You

”

