2021

啦哒网安加学院
https://edu.seczone.cn/

信息安全管理实践

企业该如何做好自身的信息安全建设和管理

目录

CONTENTS

01 企业信息安全建设简介

02 企业安全建设中的误区

03 企业安全项目案例分享

04 企业安全建设及管理

PARE ONE

企业信息安全建设简介

01

企业信息安全建设的外在因素和难点

国内的企业信息安全管理现状

行业复杂

信息安全赋能企业，面向于企业业务的关键保障.

行业、业务的复杂度导致了信息安全行业的复杂程度

割裂的信息安全经验

众多的企业的信息安全建设经验还没有被得到充分的共享

信息安全建设整体呈孤岛建设

信息安全人才的短缺

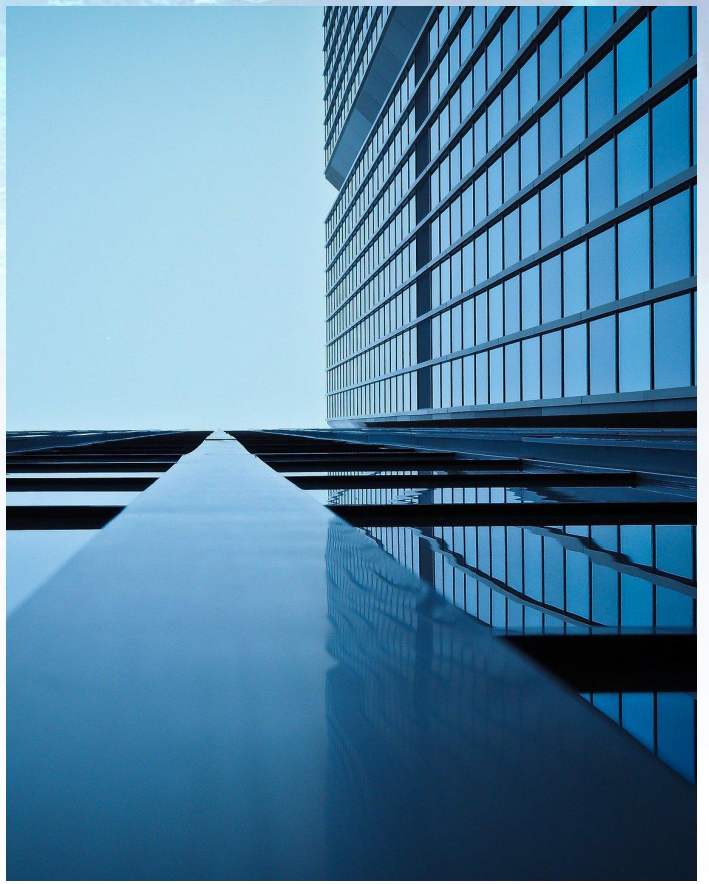
信息安全人才的短缺

信息安全领域告诉发展和人才供应程度短缺

人才地域分布的矛盾

信息安全的整体理念发展水平

信息安全建设及管理理念的落后+中国企业的发展速度



信息安全建设的战略意义

国家网络空间建设

国家网络空间领土主权的完整性

《网络安全法》中重点强调——网络空间主权是国家的主权神圣不可侵犯

行业合规监管的稳定

行业合规监管

国家关键信息基础设施的监管

商业化企业的业务赋能

商业化企业信息安全建设是为了赋能于业务

是质量管理的不可缺少的一个关键要素

PARE TWO

企业安全建设中的误区

02

传统信息安全建设误区

纵深防御

	网络	系统	应用	数据	终端
保护对象	通信网络 区域边界	操作系统 数据库 中间件	业务系统	客户数据 企业数据	客户数据 企业数据
保护要素	安全域	安全配置	开发过程 安全监测	CIA属性	CIA属性
保护机制	访问控制 VPN 入侵防范 流量清洗 流量分析 APT监测 网络准入 运维审计 安全基线 脆弱性管理 邮件网关 邮件DLP 容灾备份	主机安全基线 数据库安全基线 中间件安全基线 安全加固 运维审计 数据库审计 漏洞管控 脆弱性管理 脆弱性管理	访问控制 Web渗透测试 篡改防护 APP渗透测试 网站安全监测 源代码审核 脆弱性管理	数据防泄密 数据备份恢复 加密机 文档安全 存储安全	恶意代码防范 上网行为管理 终端DLP 终端准入 桌面管理 脆弱性管理
审计看板	资产管理 情报管理 工单管理 告警管理 响应管理 知识管理 任务管理 设备管理 用户管理 策略管理				

纵深防御中的问题和思考

1.纵深防御的维度是二维的，缺失了关于人的思考。

2.因为缺失了关于人的思考，所以没有做内外递增递减防护

3.因为没有做层次差别防护建设，所以成本居高不下

4.成本居高不下导致了没办法很好的协同业务发展

5.没办法协同业务发展所以矛盾逐渐产生

6.信息安全是企业刚需，陷入僵局循环

企业安全管理小结

传统纵深防御带有过多的技术思维

真正的企业安全建设应从商业化多角度出发：环境-资产-人-成本

安全评估及风险管理

信息安全评估的问题点。

信息安全评估参考了
传统行业的安全评估手段

风险评估计算公式：

风险值=
资产价值*
威胁可能性*
资产脆弱性

企业安全管理小结

企业安全管理建设受传统工程建设思维影响较多
应按照面向企业业务特性做建设

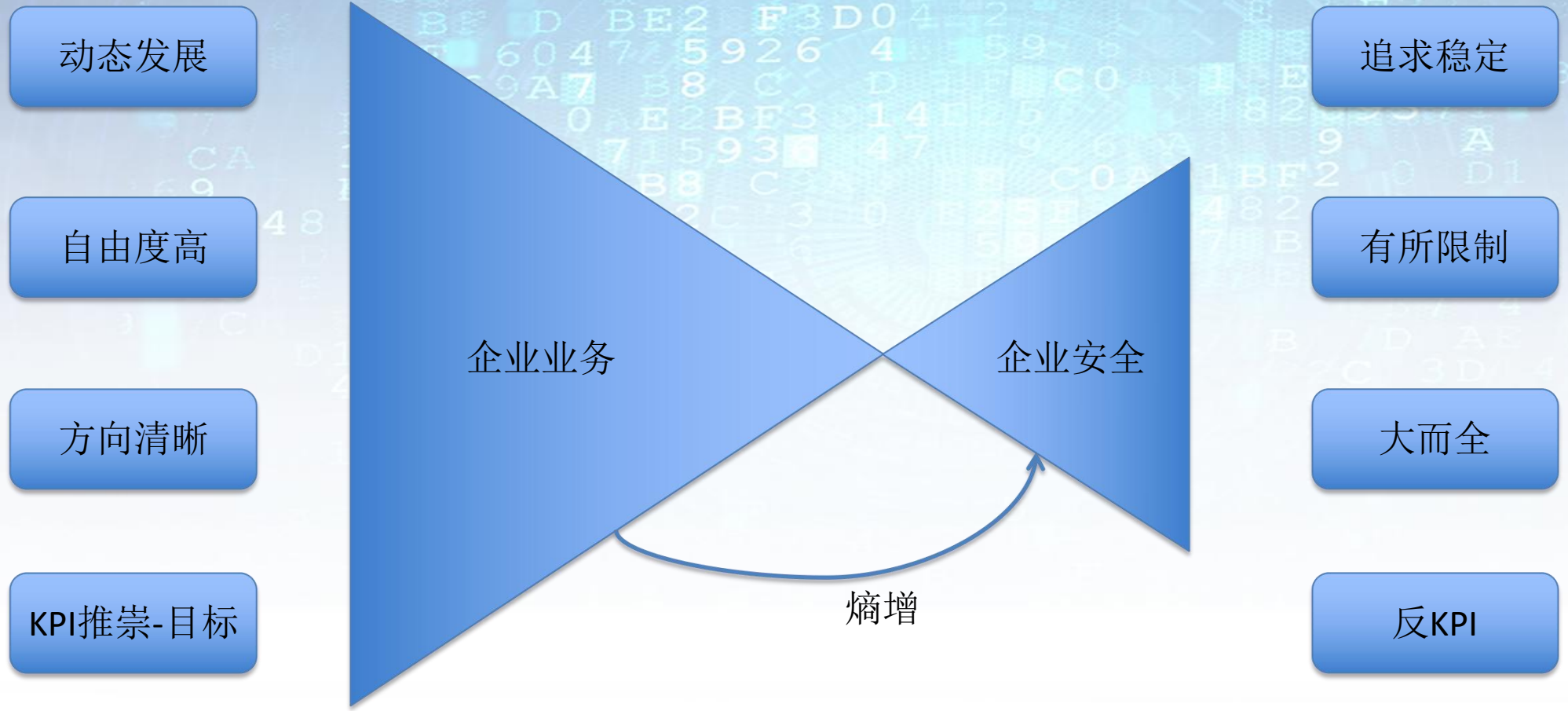
新兴行业的激进安全

一个来自18年的预判小故事

企业安全管理小结

过于激进的安全建设会导致与业务呈现喧宾夺主的矛盾
未能深度的剖析业务需求及战略发展无法很好的进行安全建设

企业安全管理与业务的方向差异



企业安全管理小结

企业安全问题是企业业务发展下的熵增必然结果
企业安全管理工作时长保持与业务相反的表征

PARE THREE

企业安全项目案例分享

03

企业安全实战项目中的成与败

来自实战项目中的思考

HW行动中的思考

为什么我们在重复的演练中

没有得到本质的提升

红蓝对抗项目思考

为什么我们按照客户要求

做的对抗项目对客户没有实际帮助价值

项目中的思考

企业建设中的“执念”，以及信息安全专业人才深度不足
先给与问题表层定性，但多数无法触及本质

项目中的思考

信息安全服务及供应商很难做到深入思考引参更多维度
仅能在技术及产品层面辅助企业增加更多成本投入

一次令人意外的进步

搞笑的演习

为应答客户的搞笑演习，
不起眼的联系表单，
看似无用的恢复顺序

宕机的NOC

遭遇双回路断电的NOC，
全片区网络及服务中断事故，
全员历时8个小时全部业务恢复

再次宕机

再次遭遇断电，
快速的汇报链路，
五分钟恢复网络，
个人30分钟恢复全部服务。

咨询服务化 服务产品化 产品数字化

PARE FOUR

企业安全建设及管理

04

企业安全建设实战心得

构建简洁弹性可持续的安全体系和机制

企业安全建设

面向合规以及空间保障

基础设施的建设

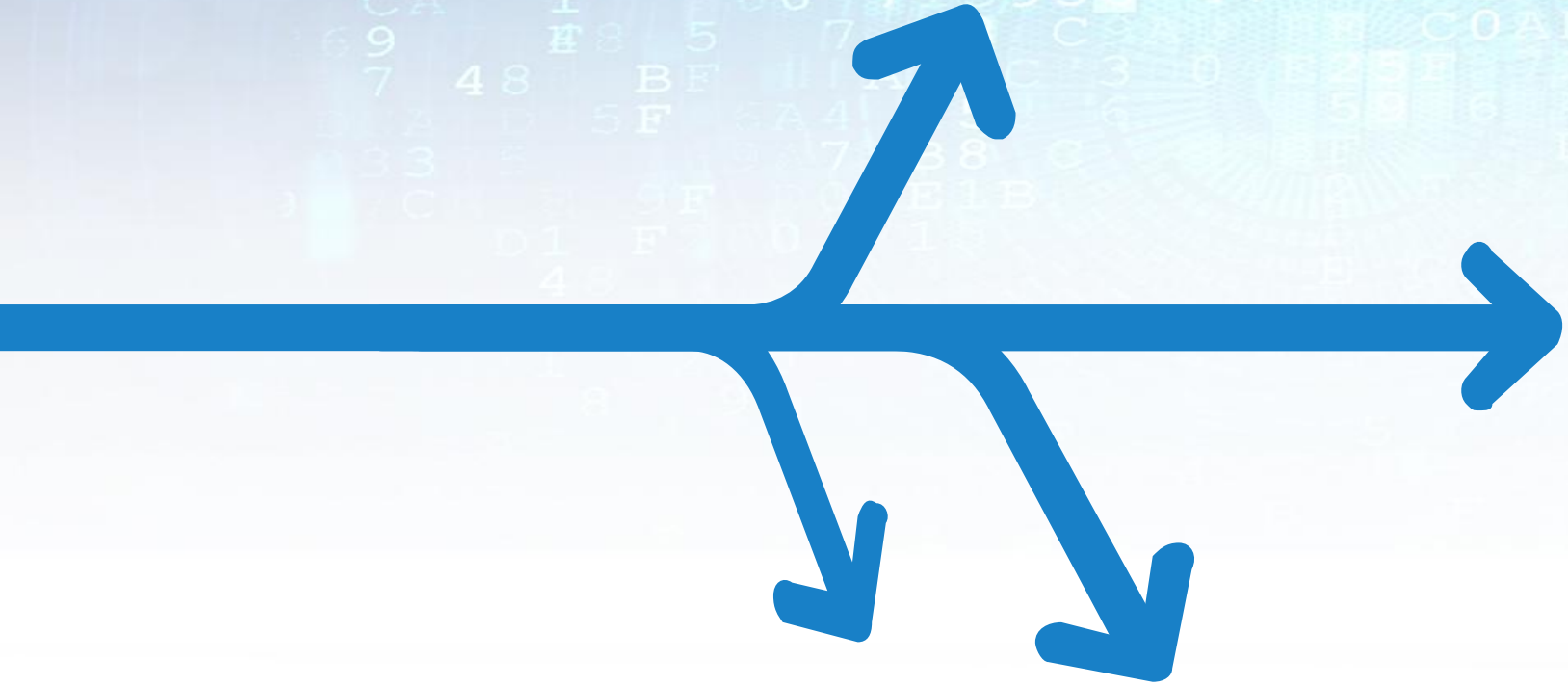
面向业务发展诉求

弹性能力的构建

构建简洁弹性可持续的安全体系和机制

将散乱的工作整合为服务

将合作模式向服务型利益协同关系出发



构建弹性管理体系

依托关键业务、重大风险、未知风险形成演练和演习。

构建弹性管理体系。

建立以治理为目标的咨询

进行业务建模、采集利益相关者风险偏好

糅合简单重复性的工作产品化

将简单重复的工作产品化

产品化带来的自由度和简洁性较好

构建简洁弹性可持续的安全体系和机制

2021

感谢聆听！