内容：我在8年经验接触实施了多个安全方面的工作。本次分享是企业角度的一个抽象化总结。主要是企业安全体系建设的方法论以及落地的逻辑思路

价值：最大的价值是我的甲方视角，甲方想法。分享过程中我也会提到一些痛点跟需求。当然更大的价值是通过我的分享内容来挖掘甲方。

举个例子，甲方有安全的需求，但是说不出来哪方面安全的需求，比如说有数据安全的需求，但是他用的这个词可能跟自己的真实需求差别十万八千里。痛点，不同行业，不同公司，不同业务痛点不同，重视程度也不同。共同的痛点是觉得乙方东西贵。

随着互联网技术不断发展，网络上的安全威胁也在不断增加，企业安全需求也随之逐渐增加。

过程大概可分为4个阶段，分别是IT建设，互联网及互联网+浪潮，黑灰产生态发展，国家干预。

第一阶段，企业的IT化建设。这时候互联网技术刚刚起步，企业刚刚开始探索互联网技术的应用。所以最先出现的应用是提高办公效率的内部办公系统，如ERP，OA，CRM系统。系统多是CS架构，服务器放在办公区本地机房。此时企业面临的安全威胁以电脑病毒为主，对应的安全需求就是主机安全

第二阶段，是互联网企业的兴起，及其引发的互联网+浪潮，然后有O2O，现在有国家主导的 数字信息化浪潮。此时，企业对互联网的探索已经成熟，互联网极大的改变了传统行业的业务形态，极大改变了人们的生活方式。互联网技术下，企业的业务开展与企业的应用呈极大的绑定状态，企业随之面临着应用安全的威胁，增加了应用安全的需求。

第三阶段，网络黑灰产也随着互联网企业的发展而发展，并急速扩张到各行业领域。比如金融，电商，游戏，通信，传媒等等。出现诈骗，勒索，水军，外挂，薅羊毛，网爆等问题。涉及数据安全，业务安全，公司机密甚至人身安全等重大问题。在严峻的黑灰产态势面前，企业增加了数据安全等方面的安全需求

第四阶段，国家下场干预。因黑灰产的猖獗，对企业及人民造成的巨大的经济甚至生命的损失，国家陆续出台了以《网络安全法》为代表的一系列通用的网络安全法规。对犯罪行为进行界定，公安部、工信部等多部门联合对网络犯罪从严打击。国家也对企业提出了网络安全能力的要求。企业随之增加了安全合规的安全需求。

抽象的来讲，企业安全体系建设的顺序是这样的。

先调研，结合法律，出方案。然后进行安全技术建设，安全管理建设，安全运营建设。

安全体系建设的第一步，首先要对公司进行现状调研。

为什么要调研，帮助企业，也帮助自己，理清需求跟状态。

除了很清楚的企业之外，一般处于不知道自己知不知道的状态，然后调研的时候，这种薛定谔状态才会塌缩成 一个确定状态。

列表的调研内容，比较粗粒度。因为高管只知道这些粗的东西。随着各方面安全建设的进行，具体落地的时候会有更细粒度的调研问题，然后去评估，去整改。比如网络是怎样划分的，数据是怎样流转的，某某业务环境的人员办公流程是怎样的等等。但是初期调研了解粗粒度的东西就够了，能够确定建设方案了。

建设方案制定时，除了公司的现状，还有一个非常重要的方面要考虑。就是法律合规。出现违法问题会非常严重，轻则软件下架，中则通告罚款，而一旦通告通常极大影响股价。重则入狱。法律法规通用的是以网络安全法为代表的网络安全信息保护方向的法律。

除了通用的网络安全法之外，国家对各行业也有特定的法律规定。这里以电商行业举例，电商行业有2019年开始实行的《电子商务法》。与电商相关联的，还有支付行业的相关法律文件。比如电商的二清规定。

电商二清，简单解释就是电商平台不能有信息二清及资金二清行为。资金清算属于持牌业务。拼多多就因二清问题被约谈处罚过，它后来花钱买了牌照。

现在结合法律法规，跟自己业务的实际情况，我们就可以制作出企业的安全建设方案了。方案中列明XXX建设优先级，建设成本等内容，交决策层审批，审批后按意见修改方案或落地执行。

技术体系的建设有全面跟完整两个要求。

全面是指安全各方面的全面，应用安全，数据安全等都要有。

完整是指各方面的技术链路的完整。每个方面的发现，监控，分析，修复，加固等技术要完整。

一般是先落实纯安全技术体系（不需要其他部分参与的），然后再落地需要其他部门配合的技术。

管理在整体安全建设中的比重非常大，安全行业内就讲“三分技术，七分管理”。

安全管理体系的建设可分为管理制度制定以及安全工作流程落地。

制度给出明文规定，安全工作流程实现制度的真实落地。

理论上所有部门的所有工作流 都可以进行安全改造。

管理制度，可以参照国家法律法规，结合公司的实际进行制定。

从高优先级的方面开始，伴随着安全建设，逐步覆盖，逐步落地。

制度跟流程跟实际的业务工作，是紧密结合的。是需要根据公司实际，进行增加或更新的。

公司引入新的工作内容，需要制定其对应的管理制度及流程，需要加入安全的考量。比如社交平台账号的自媒体推广。比如多个公司的临时工在社交媒体发布不合适言论的案例。

实际情况中，工作流程的真正实现落地都需要借助技术，借助系统工具才能实现。

安全运营体系，就是安全相关事务的持续运营。牵涉巨量的沟通，对接，跟进等工作。从安全入场，从第一次调研开始就已经涉及运营工作了。

随着安全建设的进行，安全牵扯的事务越来越多，运营的工作也会越来越多。

运营工作最难的地方，是在建设落地的过程中。去对接、说服、推进的过程。

运营工作量最大的地方，是在建设落地之后。持续使用安全设备、安全系统，处理安全事件。此时会有自动化、简单化、数据化、智能化的效果追求。

实际过程中技术，管理，跟运营是紧密结合的，没有先后顺序。然后实际安全工作的划分，有的内容也没办法按技术，管理，运营划分的这么清晰。

根据出具的安全建设方案，我们实际落地的时候，按照应用安全，基础安全等拆分，有顺序有优先级的落地。这四个方面，是公司最基础的安全方面。

按照前文的指导，他们各自都有各自的技术，管理，运营。

本次分享就只大体讲这4各方面的建设落地。

应有的类型有A,A,A,A。因为互联网对业务的影响呢，业务要么跟应用是绑定的，要么应用就是产品本身。

即使是免费单机软件/APP，有的也需要应用安全。比如PDF阅读器，打开恶意文件会导致命令执行。单机但是内置升级程序的应用，也要进行应用安全建设。如浏览器。如果公司被其他方向入侵，应用代码被插入恶意代码的话，那么所有使用此应用的用户都会被攻击。类似案例有phpstudy的后门事件,redislo漏洞。

所以有应用的公司，应当进行应用安全建设。特别是跟业务绑定的互联网应用，因为应用是最易被攻击的一个互联网目标。

采购第三方的应用，也应该进行安全评估、渗透测试等安全检查，防止别人的漏洞影响公司。

应用安全理念有 SDL/DevSecOps，围绕应用的生命周期开展安全建设。

基础安全，没有统一的定义。

基础安全的保护对象，是公司的基础资源及基础服务。会消耗的叫基础资源，不会消耗的叫基础服务。基础服务只按时间计费。基础资源有服务器、域名、ip等，基础服务有网络、数据库等。黑客可通过应用间接攻击或互联网直接攻击公司的基础资源或基础服务，因此需要进行基础安全建设。

互联网出入口的相关资源及服务首先需要进行基础安全建设，其次是内网。

基础安全建设中公有云及私有云的异同分别是

异：公有云存在资源过期问题，私有云不存在过期问题。公有云在硬件层没有实现隔离，私有云在硬件层面实现了隔离。私有云可在硬件层面实现安全加固，公有云硬件层面安全是统一的。

同：在技术体系及管理体系可进行的安全建设都是相同的。如监控，如HIDS，如操作审计，如权限管理。

围绕着生命周期展开，理念空白。

办公安全的保护对象，是公司的一切。内鬼行为，不安全的办公行为可能导致公司各方面的损失。理论上任何公司都需要办公安全。

办公安全聚焦于日常办公的工作流及公司员工。对日常办公的相关事务进行保护。

高精尖，高端制造等行业，办公安全的重要性比互联网行业更大。因为XXX

办公环境安全（网络、终端）、办公系统安全、办公工作流安全、员工安全、行为安全、身份权限安全

办公安全的理念有零信任。但是原始零信任应用的前提条件是办公系统会被大量的非公司人士，非办公区人员访问。疫情时代所有公司都出现了大量的对应需求，零信任理念也随之大火，相关产品陆续出现。

办公安全建设可借鉴零信任理念，但也视公司具体情况而定。

数据安全的保护对象是公司数据。

理论上任何公司都需要数据安全。

数据可分为 客户数据，员工数据，业务数据，财务数据，权限数据，代码数据。

数据都有结构化数据，如SQLz中的数据。以及非结构化数据，如各种电子文件及纸质文件。

围绕核心数据的生命周期展开，从各阶段提升数据安全能力。

理念就按数据安全法。