# 安全体系建设

## 前言

CSO意为首席安全官，是广义的安全，理论上包含了所有安全方面的职责，如物理上的安全（防火防盗安全生产等）、信息上的安全（广义信息及网络安全等）。CISO意为首席信息安全官，即负责广义信息网络安全。

由于传统行业的信息化改造以及互联网+等浪潮，使得其他行业很多公司都改变了业务模式，业务对网络的依赖非常严重，从而让这些公司也面临着跟互联网公司同样的网络安全、信息安全等威胁。

因此，首席信息安全官，不止需要对网络安全有深入研究，还需要对网络如何影响公司行业有研究。首席安全官下属的部门可能有网络安全部门、风控部门、审计部门等。建设广义的安全，对公司的组织结构、事务流程等方面会有相关的要求，达成条件才能实现CISO的职责。如果CISO权责不对应的话，那么广义安全就无法达成。

## 总览

安全工作开展的基本逻辑应该都是一样的，都经历以下步骤：

1. 公司分析
2. 法律法规
3. 形成方案
4. 管理体系
5. 技术体系
6. 运营体系

## 公司调研分析

安全工作中有通用部分，比如都有网络安全、业务安全、应用安全、数据安全、办公安全的安全需求。但是因具体公司行业及业务的不同，其核心关注有所不同，如互联网+社交，应用安全及数据安全是核心关注点；如互联网+金融，应用安全、数据安全及业务安全都挺重要的；互联网+高端制造，办公安全及信息安全是核心关注点。

因此安全体系建设，不能死板的按照安全理念进行，要根据公司实际情况，进行因地制宜的评估规划。根据行业、战略、业务等进行梳理评估安全风险，优先处理核心关注点，构建安全管理及技术体系。

灵活对各种安全理念进行取舍，对业务进行系统性梳理，找到核心业务，梳理业务流程，根据流程找到相关的核心应用、资产、数据等，分别分析找出其对应的核心安全威胁、通用安全威胁，分析其优先级及建设成本。

建设方案也要随时根据战略业务调整而改变，不能死板执行，要适应公司及外部安全态势。

## 法律法规

世界各国都有网络安全相关的法律规定，如中国的《网络安全法》，欧盟的《通用数据保护条例》。公司要符合法律的合规规定，按合规规定建设相关体系。

## 形成方案

结合业务及法规，可形成比较符合公司情况的安全方案。有合适的建设优先级，切合自己业务情况及战略情况。

安全体系不管是从公司角度，还是从具体的安全方面建设角度来讲，都有制度体系、组织管理体系、技术实施体系、运营体系。制度体系是指法律法规的遵守及公司内部规章制度的制定。组织管理体系是指，要设置专门的职位及部门，招聘专业的从业人员，建设及管理相关工作流程。技术实施体系是指，将制度规定与管理体系进行落地。运营体系是指，持续对安全体系进行运营。

需要注意，四个体系是相辅相成以及深度融合的，在落地过程中就需要融合推进的落地，否则单一体系落地完就只有一半的效果。

具体的建设落地一般是纵切的。先从核心业务开始，而非整个公司横向铺开。先将核心业务核心安全方面的制度规定、安全流程、技术体系、运营体系建设完成，正常运营。然后再进行其他安全方面（如数据安全，基础安全）的安全建设。然后再进行其他业务的安全建设。

## 技术体系

技术体系有全面跟完整两个追求。全面是指安全各方面的全面，完整是指各方面的技术栈完整。

技术体系建设可分为两部分，安全工作本身的技术体系及原有技术体系的安全改造。

常见的如将安全理念加入开发，进行安全开发培训、代码安全审计、安全依赖检查、开发框架安全等内容。将安全加入运维，有端口开放、操作审计、安全基线、安全配置等内容。

安全本身的技术体系，即自动化的安全监控，报警，处理等内容。

技术手段，能够自动化的互相衔接，互相配合，覆盖到整个流程的时候，就构成了技术体系。

技术体系与管理体系是相辅相成的，两者互相依赖。如管理人员的OA，管理代码的git，管理财务的ERP等常见工作系统，是纯管理的技术实现。

技术体系涉及安全支持系统的建设。只有系统才能将各技术手段自动化的串联起来，实现体系自动化。单一靠人工的方式非常损害效率，而且人工方式无法形成公司层面的沉淀，在人员离职后无法给公司留下可复用的体系。

由系统来串联技术手段，如对风险、资产、行为、人员的发现，监控，分析，评估检查，测试，处置，响应，审计，巡检，优化，感知，情报，加固，修复，安全培训等。才能实现最大效率的运营运转。

## 安全管理体系

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”。

安全管理也分为 将安全加入原有的管理及流程中，及安全事务本身的管理。

安全管理体系的建设有管理制度制定以及安全工作流程制定。安全工作流程即是落地安全管理制度。

管理制度的制定，可以参照法律法规的要求进行制定，比较有通用性。可以在制定的时候根据公司情况进行增改，添加符合公司实际的内容。比如资产管理、风险管理、权限管理、人员管理、信息管理等制度。

安全工作流程的制定，需要深入到实际的业务流程中，才能发现工作流中存在的风险。流程问题通常在安全建设的事中发现，因为事前的调研评估，梳理业务流程但通常不会进入到工作流程，但是进行安全技术体系落地的时候，会随着落地深入现办公工作流程的风险。典型的就是办公过程中的权限及行为不可控。

通常，管理需要借助技术手段才能进行落地，如XX系统。纯制度性的规定无法审计与控制相关风险，工作过程中很可能会因为各种原因而跳步骤，从而导致风控失败。

公司引入新的东西也需要制定其对应的管理制度及流程，也需要加入安全的考量。比如社交平台账号的自媒体推广。

安全工作流落地后，通常需要对其进行持续优化。使之顺畅与自动化，减少在安全节点处的处理时间。

## 运营体系

需要对安全相关系统及管理的持续运营，实现运营自动化，提高效率，提高效果。

SRC放在运营体系。

## 建设落地顺序

一般是先纯技术的落地，然后是部分运营落地，运行一段时间做出相关效果后，安全话语权得到提升，然后才能推动安全管理落地。

最初期是单一技术手段的落地，然后是单一运营，然后是单一管理。比如渗透测试及漏洞管理及运营。时间成本大概3个月。

然后是逐步补充技术手段，使构成某安全方面的体系，然后运营补充，然后推动管理的完善。比如应用安全的完善建设。这里视公司现实的不同时间有所不同，体系的完善大概1-3年时间（因为各安全方面的耦合状态，单一安全方面的建设过程中不可避免会涉及其他方面的建设，所以单一方面的彻底完善大概3年。），但是实现运转对公司的覆盖则看工作量及HC。

最后则是全方面安全的技术体系，运营体系，管理体系的落地。这里视公司情况不同时间也有不同，以下文的前4个方面算，时间为3-5年。

完整的安全体系，意味着安全体系会按理想的状态运转，能够“治未病”，在萌芽阶段就能发现处理很多威胁，善战者无赫赫之功。

## 安全方面划分

按围绕对象的不同，安全可划分成应用安全，网络安全，基础安全，云安全，数据安全，攻防对抗，应急响应等方面。下面分别是划分方面、划分依据及优先级顺序。

注意，在实际环境中，不会划分的这么清晰明确，各种安全问题之间呈十分复杂的耦合态，互相衍生，互相交叉，互相扯后腿。所以实际的安全建设中，无法彻底解决一种问题然后去解决其他问题，而是同期推进解决几种才能彻底解决其中一种问题。

## 应用安全

应用安全的保护对象是应用系统，应用系统有各种形式，Web、APP、小程序、PC客户端、物联网设备等。有互联网应用的公司，应当首先进行应用安全建设，因为应用是最易被攻击的一个互联网目标。

对公众提供服务的应用、内部研发应用、对外采购的应用，都应该进行应用安全建设。

只有免费单机软件/APP，不需要应用安全。因为它不跟互联网交互，就不存在通过应用的入侵行为。而且不收费，不存在破解盗版价值。

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。

对外采购的应用，可进行安全评估、代码审计及渗透测试，可进行运维方面的高可用架构，但是无法应用SDL理念。其他都需要进行完善的应用安全建设。

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

详情见应用安全文件夹。

## 基础安全

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。黑客可通过应用或互联网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。

基础安全并没有很出色的安全理念，可能跟理念这个词沾点边的就是“基线安全”这部分。

详情见基础安全文件夹。

## 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。

理论上任何公司都需要办公安全。

办公安全的理念有零信任。但是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。零信任对技术要求非常高，因此一般都只有大公司才能研发。另外零信任对相关办公系统的扩展能力要求很高。

详情见办公安全文件夹

## 数据信息安全

数据安全的保护对象是公司机密数据。

理论上任何公司都需要数据安全。

数据分为结构化数据，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，涉及大量的系统改造，安全产品单品有数据防泄漏（DLP），集成产品有零信任终端。

需要技术体系及管理体系合作才能比较完善的建设数据安全。单靠技术体系的话，只能对结构化数据有一个比较好的保护能力。

详情见办公安全文件夹

以上四方面，我认为是公司的普遍需求，先整理到这里。把相关文件夹都整理好之后，再处理别的。

## 业务安全

传统行业一般都有自己的业务安全体系，可能是潜移默化形成的，没有明确概念，也可能有明确概念如风控概念。

但是互联网+ 浪潮之后，很多行业的传统风控措施 在新的业务形势下不再适用，就会出现业务安全问题。比如电商的刷单、比如信用卡盗刷、比如游戏刷金等。

单讲一下刷单，它的发展链路比较长。传统商业买卖，其实形成了默认的风控规则，比如买东西讲钱货两清，讲老字号店铺。钱货两清解决了交易的信任问题。电商用中间支付解决了买家对卖家的信任问题，用7天后自动收货解决了卖家对买家的信任问题。引入的新问题是仅退款。

老字号解决的是产品品质问题，电商用成交量、金牌卖家解决这个问题，引入的新问题是才是刷单问题。

业务安全的问题，是与自己的业务形态密切相关的，不是通用安全问题。因此没有通用人才。从黑灰产来源考虑的话，也不符合人性。因为黑转白，收益暴跌。

## 安全情报

很多乙方产品内置了安全情报，也有单纯提供安全情报服务的，如微步。

安全情报可与以上几方面的安全建设进行结合，可以更具效率更具能力。结合的前提是，相关安全建设已经有了基础的防护跟检测能力，如果没有基础能力，情报就无法落地。

情报有基础类型的情报如恶意IP、域名，应用类型的情报如某组织正在对某应用发起攻击，办公安全的情报如APT情报，数据安全情报如暗网在倒卖某某数据，业务安全情报如水军攻击羊毛党等等。与应急响应也有管理，要建立相关的应急措施，如公关如技术排查。

## 应急响应

应急响应可分为狭义及广义应急响应。

狭义应急响应指单独安全部门可处理解决的问题，如运维部门发现服务器CPU异常高且处理不干净，找到安全部门对服务器进行排查处理。

广义应急响应指需要多部门配合处理的事件，如大范围基础组件漏洞redis、log4j漏洞，如window勒索病毒，需要安全-运维-开发共同处理解决。再比如业务安全的事件，如大范围薅羊毛，需要安全-风控-开发-产品共同处理。再比如用户信息泄露事件，需要公关-安全-开发共同处理，用户安抚-事件溯源-系统改进。

## 总结

应用安全，办公安全

纯互联网企业>互联网+>传统企业

一般公司的建设都是从应用安全开始的，因为应用与业务绑定，而且对互联网开放，人人都可能访问或攻击。

然后是基础安全，因为应用的关系，可能导致服务器被入侵。然后再就是网络基础设置，服务器、域名、网络、交换机，本来就是在互联网上，也时刻面临网络攻击。

再然后是其他方面的安全。

根据业务场景，建设顺序会有不同。比如高端制造业，其实办公安全，数据安全才是他们的安全核心。因为应用较少，应用也不与业务挂钩。其核心资产是自己的专利或专利落地的产品，比如芯片。

一般来说，技术体系通用性较强，发现、监控、审计、测试等等，在任何行业任何公司都是一样的。但是管理体系就不太通用，需要根据公司具体情况做建设或改造。管理体系，工作流程的安全方面，发现问题的能力比解决问题的能力更重要。