# 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（防火防盗等）、信息上的安全（专利信息，财务数据等）、生产上的安全（高危行业如化工的安全生产）、网络上的安全（互联网攻击）等。

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，首席安全官，不止需要对网络安全有深入研究，还需要对公司行业的传统安全有深入研究。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、保安部门等。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CSO的职责。如果CSO权责不对应的话，那么广义安全就无法达成。

下文内容只涉及广义网络安全及互联网模式带来的业务安全。

## 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. 行业及业务分析
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

## 行业及业务分析

安全工作在各行业、不同业务中有通用部分，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。

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。

## 安全管理体系

三分技术，七分管理。

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。

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，会随着技术体系发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。

一般情况下，安全工作流程需要有系统的帮助才能实现落地，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。

引入新的东西就需要制定其对应的管理制度及流程。 比如云，比如社交平台账号。

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。

## 技术体系

技术体系涉及安全支持系统的建设。

系统实现对风险、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。

## 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。

## 建设落地顺序

一般是先纯技术体系的落地，然后是部分运营体系落地，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体系落地。

管理体系落地后，也意味着某方面的安全建设有了阶段性成果，有了完整的安全体系。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。

## 办公安全

理论上任何公司都需要办公安全。办公安全聚焦于工作流及人员。办公安全可拆分为

物理安全：人员安全及物理资产的安全。这个方向更偏传统的安全管理，如防火防灾、防偷防损毁、防人身伤害等。高危行业一般有安全生产的管理制度跟负责人员。

工作流安全：偏安全管理，比如资产申请，权限申请。应有工作流规定，不能瞎搞。特别是对于自动化的工作流，要有审批节点，通过节点管控自动化进度。

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

办公终端安全：EDR，防病毒，零信任终端软件，DLP等

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。

## 应用安全

应用安全，大部分的应用产品都需要应用安全。

只有免费单机软件/APP，不需要应用安全。因为它不需要跟公司服务器交互，不存在通过应用入侵公司。而且不收费，不存在破解盗版价值。

操作系统、浏览器属于应用的基础设施，也需要应用安全。

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

基础安全是指，基础资产（服务器域名），基础工作系统（邮箱、OA、财务系统、禅道jira），基础网络（生产测试网）等的安全建设。

基础安全可通过安全管理，安全检查，基线设置，安全配置，安全产品等方面建设提高安全性，其中以安全产品较多。

## 数据安全

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，安全产品较少，只有一个数据防泄漏（DLP）。

## 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。

## 总结

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。

下边的内容应该拆到安全各方面里去。不在这里。

## 资产梳理管理

在各行业的现实中，资产信息类型及载体所占的比重可能有很大不同，如服务器，纸质文档，电子文档，代码，应用系统，数据库，OSS仓库等。实际体系建设中，要不断收集整理丰富自己的类型整理，拿出自己的资产表，跟具体的业务线沟通，并启发业务线发现自己的表外资产。围绕着核心资产的生态，核心资产的生命周期来进行体系化的资产发现及管理。在构建管理体系的时候，需要注意管理边界的制定与划分。

资产产出阶段：产出主体，产出工具，产出成果

资产存储阶段：存储类型，存储位置，存储工具

资产使用阶段：资产调用流转，资产形态变化

资产销毁阶段：是否可恢复，是否能销毁。

### 资产梳理统计备案定级

要对资产有梳理统计，分类分级备案，添加资产标签。做到及时更新（日更），以此为基础进行安全风险的监控，预警通知，发现处理，管控统计。

资产类型有IP类资产（服务器，负载均衡，路由，交换机，打印机等），域名资产（一级二级域名），应用资产（APP，业务系统，小程序等），数据库资产（数据库，日志中心，ELK等），云服务（OSS，CDN），代码资产（git，svn）。

落地方案：可使用云服务商官方接口获取资产信息，IDC机房资源可使用网段扫描的方式获取资产信息，办公区资产信息依赖手工统计。域名资产可使用官方接口获取所有域名数据。应用资产依赖访谈统计，联合域名资产做校对。可使用应用商店接口做APP资产监控。数据库资产信息依赖内部统计，辅助以nmap等扫描端口服务的方式校对。云服务信息依赖自行统计。代码资产可在应用资产访谈时确认，辅之以代码库项目校对。

资产管理系统，系统要有基础资产的备案、更新与离职转移功能。资产备案：归属部门、归属业务、联系人、资产功能角色、所属环境、重要性定级。资产指以上所有资产。

可根据需求与实际情况添加其他功能模块。可自建或免费使用腾讯蓝鲸系统社区版，https://bk.tencent.com/ 。

### 资产安全管理

各类资产管理方式，权限控制等，工具汇总资料：<http://www.xiaodi8.com/?id=29>

服务器登录权限管理：jump server，生产测试等环境隔离划分。

K8S权限管理：安全配置，权限证书管理。

域名管理：申请及删除机制，证书期限监控

应用管理：APP合规，APP上下架管理

数据库权限管理：操作纪录审计，权限管理，日志中心权限管理

Git权限管理：授权审计，操作审计

漏洞管理：用于漏洞生命周期的管理，通知。可使用jira，禅道等。也可使用洞察漏洞管理系统，https://github.com/creditease-sec/insight2。

SRC系统：用于接收白帽子漏洞投稿。可使用腾讯XSRC开源方案，https://security.tencent.com/index.php/xsrc。

安全分析系统：历史漏洞类型，级别，部门，数量，修复速度，安全培训成绩出具评分。

方案及需求：三分技术，七分管理。管理要借助系统才能落地。实践SDL或DevSecOps，将安全融入到项目全生命周期，措施是流程链路的打通。在项目立项、设计、开发、测试、上线、运营阶段，都使用系统工具保证各方参与，建设使用自动化流程工具实现效率，快速迭代。根据企业实际情况来落地。

资产主体管理问题：公司主体，网站主体，APP主体，有关部门备案主体，证照主体不符。

IP及域名类资产管理问题：申请或业务变更后，无人使用，资源未删除。发现安全问题后，定位不到使用人。同一资源不同业务混用，导致业务变更影响其他业务。

应用资产类管理问题：应用名录不全、无应用市场账号管理措施、无上下架发布流程管理、无应用市场名录管理。

数据库类资产管理问题：申请或业务变更后，无人使用，资源未删除。发现安全问题后，定位不到使用人。同一资源不同业务混用，导致业务变更影响其他业务。权限管理问题导致越权。

云服务资产管理问题：申请或业务变更后，无人使用，资源未删除。配置措施不满足安全实践。账号管理问题导致账号遗失。

代码资产管理问题：项目分支混乱，代码合并问题，项目管理权限，项目管理问题。

工作系统，运营系统，后台系统账号管理问题。

权限分配及备份问题。

## 安全检查

针对以上资产的自我安全检查，扫描，渗透测试，监控。

针对以上基础资产建立安全扫描与监控机制。

针对IP类资产，主要关注漏扫及对外开放的端口监控。

针对域名及应用类资产，主要关注应用漏扫及渗透测试有效期，上线版本监控。

针对数据资产类资产，主要关注弱口令，访问控制，操作审计监控。

针对云服务及代码资产，主要关注信息泄露，代码审计。

落地方案：使用msscan、openvas、商业化漏扫，安装MySQL-audit插件进行SQL操作审计，GitHub代码库监控。

<https://github.com/madneal/gshark> GitHub及gitlab监控https://paper.seebug.org/1560/

<https://paper.seebug.org/1627/> 巡航扫描

<https://github.com/HXSecurity/DongTai/> 被动扫描

自动化安全测试：http://www.jrasp.com/

建立健全针对以上资产的渗透测试机制，最好能够实现应用上线前的渗透测试以及红蓝对抗测试。可使用IAST方案集成到功能测试中。https://github.com/HXSecurity/DongTai

安全隐患：敏感服务对外开放，弱口令，服务及框架漏洞（版本），服务器基线，服务器直连，过多的服务器间ssh互通，云服务配置不当，服务器防病毒。

解决方案：基础安全扫描与监控，基础安全防护的安装，Jump server等对服务器的集中管控，建设云服务安全配置的巡检机制。

业务及应用安全：内容包括薅羊毛，代码安全管理，账号安全，交易风控，征信，反爬虫，反作弊，人机识别，反欺诈，反钓鱼，垃圾信息，内容安全，黑灰产等。

这个要看具体业务场景进行分析。可在SDL过程中，项目立项之后就去研究是否有相关风险。自己做过薅羊毛跟反爬虫的研究。

业务风控：同地址，同手机号，同身份证号。阿里有手机号风险检查

接口安全测试：api自动化测试。https://github.com/flipkart-incubator/Astra

可使用python的自动化测试框架pytest，手写自动化测试用例。这种方式只能检查 应用安全问题，如越权，信息泄露。无法检查XSS，上传，SQL注入，组件漏洞等。无法检查业务安全问题，如促销活动的薅羊毛，如冒充新用户，如刷单。

依赖包检查：周期化依赖包检查。

Go:https://deps.dev/go/github.com%2Fgo-kratos%2Fkratos%2Fv2

Java:https://mvnrepository.com/

Python:https://www.cnnvd.org.cn

容器安全检查：trivy

镜像安全：按照最佳实践 https://dockone.io/article/8828，进行镜像的检查与选取。

镜像扫描，在 CI 中 使用 https://github.com/aquasecurity/trivy#gitlab-ci 进行容器安全检查。华为云提供镜像安全扫描，但是目前仅支持“华北-北京一”、“华北-北京四”区域。

## 安全加固与保护

Istio启用安全功能

K8S安全配置

软件覆盖率，正常率，误报率

购买或采用开源安全设备进行以上资产的安全防护，提升防护的基线水平。

IP类资产防护：制作满足安全基线的镜像，使用安全镜像新建服务器。使用堡垒机、jump server等控制登录及做安全审计。安装HIDS软件（AgentSmith-HIDS，ossec，安骑士，青藤云）做服务器安全审计及监控。安装防病毒软件（商业HIDS自带）。

域名及应用资产防护：可使用WAF、高防、SSL服务进行域名防护。使用加壳加固、混淆加密服务进行APP防护。

数据库资产防护：用户及权限管理，访问控制，操作审批及审计，依赖规章制度及监督执行。可建设操作中心，操作中心具有记录审计功能，统一使用操作中心进行操作，方案参考云数据库DMS服务。

云服务防护：注意安全配置及权限最小化使用，注意资产管理。

网络设备的保护：防火墙 (Juniper FW)，IPS/IDS (Suricata/Snort)，DPI (Bro)，堡垒机，Web代理网关(IronPort)，邮件网关(FireEye/IronPort)，DNS RPZ，VPN，WiFi等；

网络架构的保护：NAC，SDN，ZeroTrust (类似于Google的BeyondCorp)，VPC等；

服务器／办公电脑的保护：反病毒，EDR，HIDS/HIPS等；

移动终端的保护：MDM (VMware AirWatch)等；

物理门禁的保护：异常警报，访问日志，监控摄像头等；

业务系统和服务的保护：SDLC (包括安全开发规范以及相关的自动化工具、流程、平台的建设)，VRP (漏洞赏金计划)等；

业务数据的保护：数据分类标准，数据处理标准 (传输和存储)，数据共享要求，合规管理要求，业务风控体系，通用安全系统和组件(KMS, 统一认证和授权平台，AAA)等；

### 办公区网络

安全隐患：WiFi密码爆破，WiFi万能钥匙，办公区自建网络节点，办公设备安全（个人PC，非个人办公PC，打印机，路由，交换机），内部泄密，病毒远控，内网攻击。

解决方案：网络准入系统，域控，划分VLAN，安全意识培训，设备安全配置及管理。有些隐患并不能通过纯技术方案解决，还需要有管理运营。

内部泄密：数据防泄漏（DLP），上网行为管理，安全意识培训，签署保密协议

终端防病毒：工作电脑预装防病毒软件，辅之以安全意识培训。

攻击识别：采购威胁感知设备。安装域控之前，内网攻击一般由病毒蠕虫从办公设备发起，无特定攻击目标。安装域控之后，内网攻击都会重点攻击域控。

### 线上区网络

安全隐患：生产、测试、办公区间的访问控制，线上攻击。

解决方案：各环境之间的实施网络隔离，做好办公区网络与线上网络的访问控制。对于物理机房，可以采购IDS、VPN、防火墙做网络边界管控。对于线上攻击，可以采购高防、WAF服务。建设SOC，**SIEM**平台对攻击进行报警与分析，还可以建设蜜罐服务，用于探测内外网攻击。

组件部署，信息采集，信息分析，信息展示。

## 感知与审计

针对以上资产的安全态势感知。发现攻击，发现威胁，报警。操作记录审计。

服务器端口监控：<https://github.com/awake1t/linglong>

域名安全扫描：crawlergo

蜜罐：内外网

华为WAF的报警

Git 操作审计：仓库拉取数量报警。仓库组权限配置报警。

Git权限审计：仓库及员工授权表

服务器：jump server 服务器操作审计

GitHub监控：<https://github.com/madneal/gshark>

安全情报：<https://github.com/virink/VulWarning>

安全埋点：在系统上进行安全埋点，统计数据。

对资产的异常监控，及时发现资产安全状态。

主机的HIDS、安全DNS再到威胁情报等，安全监测的Sensor类型不断扩大。

除了这些安全设备之外，各类被保护对象的应用日志也是非常好的Sensor感知器，比如说AD日志、邮件日志、堡垒机日志，甚至是门禁日志，EDR日志等都非常有用的。应用日志配上简单的规则就能发现非常多的异常，但要求日志本身记录的完备性。

日志审计：

异常行为监测：<https://falco.org/zh/docs/>

<https://blog.51cto.com/u_15315026/3206959>

<https://github.com/hidd3ncod3s/sysdigfalcorules>

<https://github.com/sysdiglabs/falco-analyzer>

<http://www.catddm.com/archives/769>

多组件介绍https://www.1024sou.com/article/522111.html

等保合规等

## 运营与安全管理

安全风险展示与管理。

安全防护框架的目的是尽可能多的部署有效的安全感知器Sensor，这些安全感知器构成了信息安全的一个天网。这部分是最基础的工作，也是传统安全的主战场，需要历经多年的持续投入、积累。安全Sensor的部署应遵循纵深防御的理念，安全Sensor会产生大量的监测日志，作为安全运维框架的输入。

之后建立SOAR，持续自动化响应的运营体系，实现感知，审计，处理的自动化。

确定运营流程，设计运营系统，任务分配。

持续运营安全服务以及安全系统。资产系统、漏洞管理系统、SRC系统，高防、WAF、应急响应、安全合规、渗透测试等基础安全服务。

数据统计通报，WAF报警数量，GitHub监控数量，安全情报数量，等可视化工作。

## 安全规章制度

制定安全相关的规章制度，配合安全建设。

落地方案：按照安全建设计划出具安全规章，保证制度出具之后能有效监督执行，能与安全项目有效配合。

### 法律法规：

《中华人民共和国网络安全法》：网络的安全顶层指导文件。

《网络安全等级保护条例》：《网络安全法》的重要配套，需要第三方有资质的公司对业务系统进行等保定级。主要流程为：确定定级对象→初步确定等级→专家评审→主管部门审批→公安机构备案审查→最终确定的级别。

《信息安全技术 个人信息安全规范》：针对个人信息收集及使用的规范性文件，主要着眼于APP的 “强制索权、捆绑授权、过度索权、超范围收集”等问题。

《关于开展APP违法违规收集使用个人信息专项治理的公告》：针对APP的专项行动，网络安全法的具体落实检查行动。主要着眼于APP权限，个人信息收集两方面的合规。《App违法违规收集使用个人信息行为认定方法》为具体检查项，可根据《App违法违规收集使用个人信息自评估指南》进行自评估。

《数据安全法》：主要着眼于企业数据安全建设。要求企业建立安全管理制度，使用防病毒，防攻击，数据备份加密，实施审计监控等技术手段保护数据安全、内容安全。建立健全应急预案，用户信息保护，投诉沟通机制等基本制度。

《个人信息保护法》：主要着眼于用户个人信息保护。要求企业最小范围收集，最小权限使用用户信息。企业要尽到用户信息保护的义务，做好分类分级保护、加密等。企业要公开公正，透明使用用户信息，不能大数据杀熟。企业要充分尊重用户意愿，用户拥有要求注销删除的权利。

《网络产品安全漏洞管理规定》：要求企业建立SRC并有效长期运营，建立健全SRC奖励机制对漏洞报告者进行奖励。

### 内部规定：

《员工手册》：

《安全事件应急响应预案》：。

《App隐私合规设计规范》：已提供并应用。

《SRC标准》：。

《数据分级与等级保护》

《数据防泄漏规定》

《基线及中间件安全配置》：K8S，dockers等配置指南。规定敏感服务。

《云服务安全配置指南》：云环境安全

《服务器管理-系统安全管理规范》：

《信息安全规定》：

《Git安全使用规范》：

## 内部监察

防泄密，防内鬼等。

## 攻击阻断

针对攻击的阻断，报警，处理。证据留存。

## 网络舆情

脉脉舆情，暗网监控