大家好，这篇是系列分享第五篇。之前的分享请移步我的个人主页查看。这篇来分享一下数据安全建设的落地实操。

## ****落地准备****

在进行实际的数据安全工作落地之前，有两方面的准备工作要做。一方面是思想准备，一方面是落地的逻辑方案准备。

### ****思想准备****

先说思想方面的准备。我们知道，网络安全的建设工作，不是安全部门自己能完全cover住的，安全部门发现问题，但是问题的整改，还是需要其他部门进行落地整改。不管是整体企业的网络安全建设，还是单一方面的安全建设，都是需要多部门协同配合的工作。

数据安全的建设更是如此。数据安全，其牵涉的部门是全公司的所有部门。而且数据安全的实施各阶段，梳理、分级、加密、防泄漏等，都绕不开各部门本身。因为信息数据是所有部门的工作要素之一，也是部门工作的产出之一。只有各部门自己，才最清楚自己的数据，清楚数据的生命周期，知道从哪里产生，如何传输，如何存储，如何流转，是否共享，是否备份，是否复制，是否有数据产出等等。

而多部门的协同配合，在任何项目，任何工作，任何公司，都是一件很麻烦的事情。为了解决其中的麻烦，国外最早出现了PMO这个角色，国内有些大公司也开设PMO岗位。但是对于一些中小公司，就没有专门的PMO了。

所以中小企业的安全部门，要自行去推动其他部门进行安全建设的配合与落地。

安全部门扮演了整体公司安全事务的领导者的角色，但是没有领导者的权限，也没有人去帮助安全部门推动其他部门进行协同落地。

这些事情都需要安全自己来做。

数据安全相比应用安全，更加需要沟通能力、说服能力、耐心等等技术之外的能力，去把事情讲透讲清楚，把价值跟必要性讲明白。

所以工作开始之前，要有心里相关的心里预期。

除了以上心里预期之外，还要有另外一个数据安全生态的认知。

那就是相对于应用安全及基础IT设施安全，数据安全是一个新兴生态。里面的安全从业者，方法论，工具等都是非常贫乏的。比如应用安全，有burp，sqlmap，waf，扫描器，代码审计，字典等等工具。基础安全，有NMAP，osssec，hydra，nids，onlydebug等等工具。数据安全的工具，就数不出来几个了。数据安全里面，我们需要帮助数据梳理的工具，有帮助数据分类分级的工具，有帮助数据解析（AI关联价值分析）的工具，有帮助文件解析的工具（非结构化数据），然而市面上，其实并没有这些工具。当然，可能有数据安全的从业者有一些自己的脚本积累。

另外，乙方产品里面，数据安全的产品，最成熟的是数据防泄漏的客户端。而数据防泄漏，只是在办公终端，数据链路的最末端对数据进行安全防护。它并不覆盖数据仓库，也不覆盖数据生命周期。也有乙方公司研发了整体数据安全系统的产品，但是其研发思路，还是基于应用安全/基础IT设施安全产品的思路来进行的，依赖流量镜像分析，这种思路与模式，完全无法满足甲方的需求。

而且，因为数据安全本身的工作特性，其生态发展也是缓慢的。数据安全对从业者能力的要求，要求更多的是体系化能力，而非数据生命周期的技术能力。举个例子，企业是否需要一个密码学的专家来开发一个新的加密算法？一个密码学专家，会选研究机构，国家，巨无霸集团，还是普通企业？

### ****方案准备****

另一个方面的准备，是落地的实操方案准备。

准备内容除了之前两篇文章讲的内容，还需要更细的实际落地的方法论。

即我们要知道，数据安全建设里边，更细节的整体的落地的工作内容有哪些，数据生命周期的落地内容有哪些。如安全部门负责什么，其他部门负责什么？生命周期的各阶段，什么部门需要做什么事？这些事，对于其他部门的价值是什么？他们为什么要配合？哪些东西是安全的底线，哪些东西是可以跟部门商量的，如何跟其他部门沟通配合，如何实操落地工作内容等等等等

## ****落地实操举例****

这里举例一个实操过程，欢迎大佬们指指点点。

### ****应急及领导的需求调研处理****

在整体企业建设方案制定的过程中，我们调研了公司层面是否需要安全应急，以及公司层面有没有什么迫切的安全需求。

安全事件应急，以及安全需求可能对应着数据安全这个方面。

这时候我们需要评估，这些事务是否是能够短时间内处理掉的东西。

如果是个短期能处理的东西，就先处理这个。如果是需要体系化建设才能处理，才能满足的需求事务，那么它就是一个长期的工作。那么就应该把具体的事务放到整体建设方案里。优先级调高。

### ****熟悉人员****

数据安全的落地建设，我们需要认识公司所有部门的领导。

可以请领导带着安全跟各部门的领导认识一下，简单对齐一下信息。留一下联系方式，便于后期的沟通以及工作开展。

### 数据安全组织建设

数据安全治理组织的建设，应该是数据安全治理中首要的工作。通常是建立虚拟组织，人员组成有公司高层以及各部门负责人。要有公司明文的制度规定，明确各人员的权责划分。

一方面，从法律合规上讲，《数据安全法》规定了公司必须要有明确的制度，组织，人员，职责划分，要有健全的数据安全保护体系。

另一方面，从数据本身的特性来讲，数据安全的落地，必须要由公司高层及各部门的支持。

有了上层支持和完整的数据安全制度，才能顺畅的推动工作，否则处处都是阻力和难以翻越的大山。

### ****宣讲会****

认识各部门领导后，找时间把所有领导拉到一起开个会，讲一下公司要开始进行数据安全的建设了。

会议应该讲清楚为什么做数据安全，它的意义价值是什么。数据安全建设的方法论是什么，在接下来的实际工作中，内容顺序是什么，安全负责什么，其他部门负责什么。各个业务的优先级顺序是怎样的。

宣讲会的目的，是安全跟大家对齐一些信息，让大家心里有个谱，方便后续的配合协作。

### ****确定沟通协调机制****

数据安全会涉及到大量的，比应用安全还多的需要配合的工作，沟通会比数据安全更加频繁。因此可以让领导们在自己部门里定一个安全的对接人，安全部门后续的会议，跟一些工作的对接，可以找这个对接人来做。

### 数据****梳理****

数据梳理是落地执行的第一步，是数据安全治理的基础。数据安全治理需要对公司的信息数据有清晰的了解，因此需要进行数据梳理。又因为数据特性，只有其他部门自己才能梳理自身的数据，并给出价值分析，使用场景及排序等信息。

数据安全治理是一个长期过程，不是一蹴而就的。因此，数据梳理也建议分期进行。先从高优先级部门，高优先级的数据开始。数据类型先从结构化数据开始。一期一期推进，持续安全运营。

### ****建设组织人员变化的发现能力****

安全部门应该建设组织变化的发现能力。

发现变动，安全部门有责任去跟新的部门及人员对接，将之纳入到数据安全体系中，确保数据安全的覆盖是完整的。

能力建设可以通过管理方面，在工作流程上做一些建设，让人事部门在有相关变化的时候及时通知安全。

也可以通过技术方面，进行一些监控建设，通过公司组织及通讯录变化发现人事变动，调整数据安全相关的制度，组织等，与新部门新员工做好对接沟通。

### ****方案制定****

在数据梳理完成，优先级确定好，数据使用场景明确之后。

安全按优先级，针对具体数据情况及安全建设情况，制定细化的安全建设方案。确定其具体数据适配的安全措施。此时应该将法律法规纳入考虑范畴，判断什么数据需要进行合规处理。

### ****具体方案讲解****

需要跟数据的相关部门，涉及的其他部门的工作实施人员，讲解方案。

讲好安全要做什么，技术这边的人要做什么。优先级是什么，时间预期是什么。这样方便实施人员事先了解，以进行工作安排。

### ****落地执行****

跟进工作的落地执行。数据安全工作中，具体数据的拆分，迁移，系统改造，加密，脱敏等落地工作，大部分是由其他部门配合才能落地的。

对于单条数据，工作有采集，传输，存储，使用，加工，销毁的生命周期内的安全保护。

对于整体的数据安全，应该建设整体的安全管理与运营体系。比如如下系统：

统一的数据信息备案系统，智能化自动化的分类分级系统，统一的数据权限申请系统，统一的安全监控审计系统，统一的安全管理及运营系统，统一的培训考核系统，统一的流转视图展示系统等等。

### ****持续运营****

要对数据安全进行持续运营，比如以上系统的运营，安全设备的运营，跟进漏洞修复，跟进更新，跟进新项目等等

### ****合理分配资源****

安全建设要注意合理的分配资源。

在针对某应用的安全建设到达一定水位后，最好将资源投入到其他应用中。

在整体数据安全建设到达一定水位后，最好将资源投入到其他方面的安全建设中去。

这样处理，能够最大发挥资源的性价比。快速拉升整体公司的安全水位。

## ****总结****

数据安全更加依赖部门协作

数据安全生态较弱，工具较少

最好提前争取高层支持，建立好公司内的数据治理组织

安全要把安全事务分配好，领导好，做好安全建设的领导工作

方案提前讲好，让其他部门有数

建立好沟通协调机制，随时沟通，及时信息互通

安全意识的培训培养

注意投入产出比，灵活配置资源。

## QA

弟弟失业中，目前在上海，正在找工作。

大佬们如果对我感兴趣的话欢迎加我VX：qinbingjie1101。普通交流，扩展圈子也是可以的 ：）