==Ph4nt0m Security Team==

Issue 0x02, Phile #0x03 of 0x0A

|=----------=|
|=----------=[CSO的生存艺术]=----------=|
|=----------=|
|=----------=|
|=----------=[By ayazero]=----------=|
|=----------=[<ay4z3ro_at_hotmail.com>]=----------=|
|=----------=|

本文主要面向管理人员，对于有特殊需求的技术人员可适当参考。

引子：

偶尔看到一篇文章《2008预测技术派CIO面临失业》，其中“预测指出2008年对那些专注于IT运营和成本裁减的CIO来说将是一个转折点，CIO必须证明他们作为商业伙伴的价值，否则就会被打入冷宫。报告还指出现在许多CIO还埋头扎堆于"技术丛林"中，却对战略管理、业务营运、财务融资、人际关系等一知半解，这都将会面临被淘汰的困境中。随着企业的发展，传统技术派 CIO已经无法再胜任高层管理工作，如果还一直只专注于技术的角色，将与战略化的角色不符，表示CIO已经不胜任高层管理岗位。而且传统技术型CIO通常还会忽略一件极其重要的工作，就是对公司运营现状和管理需求的不甚了解，使IT部门只成为一个信息技术中心，而不是管理信息的中心。实际上，只有与管理、业务相结合，技术才能有用武之地，否则只能导致闭门造车，当技术脱离业务时，再好的技术也徒劳无益。

事实上，一位IT技术专才和一个合格的CIO之间是存在着巨大的差别，技术和管理几乎完全是两个领域：管理对人、技术对事;管理贵在均衡、技术追求完美;管理看宏观、技术重细节。一名IT技术人员即使可以做好研发管理、项目管理、甚至IT部门经理，但要想成为在残酷市场竞争下生存的CIO，就必须改变其思维和言行举止，经历更多的磨炼。一般来说，传统技术派CIO有以下几个难以逾越的障碍。

(1) 只关注技术，业务知识面窄
(2) 团队协调管理能力弱
(3) 人际沟通协调能力不足
(4) 技术精英的清高与孤傲

其实成为一名CSO本质上和CIO是一样的，对于个人而言最重要的是解放思想，切勿固步自封。本文涉及的内容是管理人员必须考虑的，是技术人员可以借鉴的，是有志于进一步提升的人需要理解的。这些都是“术”而不是“道”，懂得“道”的就不用看这些了。

我认为CSO需要三种技能：智慧、管理、技术，Cobit、ITIL、7799等一大堆安全治理标准虽然是站在了管理的维度，作为一名咨询顾问应该是可以了，但是对CSO来说是绝对不够的，你还需要一种能力叫做智慧。“以智治国，国之贼也。”我说智慧并不是提倡“人治”，我们的最终目标肯定是要建立一个和谐的法制环境，但是安全标准仅适用理想的法制环境，而这个环境的建立和推动需要的正是智慧！诚如我在《信息安全的职业生涯》中所言，建立安全标准、策略、程序等都是相对简单的事情，在组织中成功开展工作最大的能力是EQ，尤其对于国内的企业而言更是如此，力挽狂澜建立法治环境需要的是CSO的情商。指望老板把信息安全捧在手心为你铺石开路这个出发点本身就错了，因为君王没有为臣下服务的义务！只有当你的“建议”非常合理、切中要害时，他才会为你提供资源。

1.为什么不重视信息安全

这是一个被谈及太多的问题，我觉得我们应该尝试理解一下自己的老板。为什么平时一个销售跑过来大吹特吹的做一番售前演示，而你根本无动于衷，好像对牛弹琴一样，因为没有切中要害。当且仅当博弈发生在同一个层面时，博弈才是有效的。在MBA的教科书案例中，企业危机通常都源于战略选择和治理结构等问题，信息安全往往还没有进入高层管理者们的视野。现实生活中有不少信息安全做的不好的企业仍然大受投资者追捧，华尔街的分析师都推荐高价买入，因为他们看的是财务报表而非IT审计报告。信息安全固然重要，但是它通常排在战略、人力等一堆名词之后。扪心自问我们说安全重要很大程度上因为我们自己是做安全的，综观我们的知识体系结构，是不是安全占了主导呢？因为双方的信息不对称，视点不对称，思维方式不对接，使得我们在观点营销的过程中处于弱势。

但是信息安全确实很重要，游说是必不可少的，因为这是CSO的职责所在。

舌战群儒，嘴吞六国岂是一日之功？说服高层管理者对于CSO的知识背景和能力来说是一个很大的挑战。CSO的内涵应该是多层次、多维度的。实际上，与老板对话说明安全的重要性往往不在于你那些安全或是风险管理的知识，呵呵~

另一方面，我们嘴上要坚持说“安全”的事，但心里要想着所有的方方面面。如果你只想着安全，就说明你已经思维定势。

记住：CSO不只是CSO！

我们看那些菜鸟销售总是见了面还没听客户需求就开始卖东西了，而那些老鸟则是先做朋友，然后卖你东西还是为了“帮你解决问题”。

这说明一个很重要的问题：博弈的角度不对，也许你换位思考了，但是考虑的还不够，就好像你明明知道千米之外有一个目标可是云雾缭绕，你就是看不清靶心在哪。

要解决这个问题，首先要不断让自己的知识重心向高维度和多平面迁移，例如有时间可以看一些经营管理方面的书，尽可能的熟悉公司的业务，多看一些分析师，投资者，专家对本行业的评论，多培养自己的逆商AQ，知道你的上司、老板的业绩压力是什么，知道他们的痛处，很多时候出台一个什么政策，让你去做一个什么策略，写个什么文档，往往只是表面现象，背后另有深层次的原因。如果不闻不问按自己的理解往往会对不上需求，切勿闭门造车。等EQ攒到了一定程度，自然临渊而知深浅，闻一而知三。

2.极端强势的作风

有人奉行强势的策略推动,有一句广告词叫“刚柔并济,以退为进”太强势了反会伤了自己。当你把所有策略一下子推出去的时候，当你爽的时候一定有很多人不爽。有句话叫“水至清则无鱼”，往铁板上狠狠使出一拳，自己也会痛的。强势的策略推动还源于另外一种心理，即他认为所有安全策略均是合理的，别人都是不安全的典型，都应该抓了打PP。其实这是本位主义的表现，试想没有那些业务部门还怎么会给你这个就业机会呢？有些问题从你的角度是对的，但从别人的角度未必是对的。敬业，其中一点就是要有大局观。我们的最高目标是要实现股东利益最大化，所以有时候应该适当折中、甚至妥协退让。为什么要退？以退为进！很多人都想让信息安全具有影响力，又不懂得因势利导，欲望和信仰不统一，自然只剩郁闷。

例如：在会议上，不要急于表达安全策略的具体内容，应该倾听业务部门的“牢骚”，分析他们的牢骚的原因，从而变通策略的形式或者暂时搁置在所有的策略文件中，要非常注意措词，在发送邮件前，要仔细斟酌，不要逞“快”，一定要站在阅读者的立场揣摩一下对方的心理。推策略尽可能通过流程，而不要把自己放在炭火上烤，是安全职能向公司的业务推策略，而不是你在向别人推策略。

3.过分弱势的作风

反过来，如果CSO缺乏智慧，整个团队必定弱势，更不用谈那些分蛋糕的事情了。

4.“借势”而行

孙子兵法曰“如转圆石于千仞之山者，势也”，向人借势，向事借势。站在高山上，那是势。有时候没法站那么高，即使在平地上，如果临千尺之渊，你也自然有了势。信息安全事件/事故是我们不愿意看到的，救火奔命是消极的一面，但积极地看，这是可以大肆借题发挥的机会。往往顺风望去，此时你就在高山之上，而别人就成了千尺之渊下的鱼。出了问题，自己不要躲起来，而是要把号令百军的旗帜树起来！很多事情，让自己换一个思考方式，让别人也换一个思考方式，结果马上就变了，权变再权变，变通再变通，引导再引导，刚才千里长江东逝水，现在马上滔天巨浪向你涌！能否站在浪尖上取决于你是否能因势利导。就好像曾国藩说“屡战屡败”后来又改成了“屡败屡战”。看~一个字都不换，稍微变通一下结果就完全不一样了！

例如：安全事件发生时你可以以退为进的暗示：人、流程、技术上的一系列问题，以及资源的不足。在关键事件响应之后趁势抛出一堆诸如BCP（业务持续性计划）的流程，有些东西不是第一次抛出马上就会被管理层接受的，接而第二次、第三次……对方的感性认识也有个过程。

5.中庸

中庸，这应该是精髓了，这是笔者所提倡的做事方式。中庸的正解是“恰到好处，和谐圆融，不偏不倚”而不是妥协退让和毫无特点的代名词。中庸应该是在企业内推行信息安全及风险管理策略时的主基调，掌握了中庸，你就超越了CSO其实中庸是符合风险管理理论的，风险承担和价值收益的关系是呈正态曲线分布的，承担过高的风险，或过低的风险（过多的控制从而影响了盈利效率）都是不恰当的。恰如财务杠杆，维持适当的债务可以减税从而提升股东价值。总的来说我们应奉行：“坚持原则，以退为进”该唱红脸时也当仁不让！

例如，当你只懂安全而不懂业务时，开出的药方往往是“过激”的。所以呢，一定要熟悉业务，应该是当你的策略出来的时候你就已经知道“控制”会对生产经营环节产生多少影响，大局观不仅依赖于你的“意愿”，还依赖于你的“能力”。此外，多聆听业务部门对ISMS的反馈，这样你才可能越来越恰到好处。所以不只是沟通的形式重要，沟通的内容更重要。

6.奉天子以令不臣

让其他部门遵循ISMS的标准是一件不太容易的事情，第一步就是要“奉天子以令不臣”，这也是ISMS中要求管理层签署发布信息安全文件的原因，只是单纯的靠文件是不够的。具体还体现在做事方式上，把水流重定向，让他们流到老板的大山脚下去，可别把你这座小土堆给淹了。但是，不能屡试不爽，因为老板站在他自己的角度要追求的也是“平衡”，切不可有了一点小事就往老板那里推，那样的话就显得你很“无用”。

注意：这里用的是“奉天子以令不臣”而不是“挟天子以令诸侯”，后者是行不通的，而且会有很大的反作用。

不管你说“洗脑”还是“忽悠”，目的都是一样的，建立风险管理的“共同语言”，让别人的思维方式顺应你所建立的“模型”，这样才方便与管理层对话，甚至主导思维过程。在我看来给管理层的培训远比给普通雇员的培训重要，因为在企业里，只有自上而下的“营销”才是可行的，反之只会力不从心。

7.深入关键业务，利润中心

为了显现信息安全的价值，我们的工作首先要与关键业务绑定，凡事分轻重缓急。不深入应用，停在表面做技术平台的安全是没有价值的，OS，数据库，代码等等只是业务的承载媒介，只是IT基础设施，他们并不是业务本身，真正重要的是信息，是数据！这也是信息安全前面那两个字的含义。理解了信息，你才真正清楚自己在管理什么。

8.IT，是对人的流程和对技术的架构

之前说过IT，Information Technology是一个复合词，是信息+技术。操作系统、数据库、代码这些属于T，属于技术平台如果只做这些，那么尚处于外围，只有当你贯穿企业内部的价值链、整合产业链上的信息传递做安全管理的时候，信息安全才可能被提到战略高度，否则安全就是一个可以外包的边缘职能。最简单的理解信息安全=人（权、责)治理+事（流程，程序，操作指南）+技术（标准、策略）坐在办公室里，闭上眼睛，马上能想象出公司所有主营业务的数据流向（包括第三方）的时候，就能理解如何利用现有的“安全技术”来保护企业的“信息流”。

9.创建治理结构，变人治为法治，但仍需要变通

这是信息安全的核心，创建一堆标准、策略是简单的事情，但是让雇员都去遵循，不是遵循一天，而是持续的自觉遵循是困难的事情。建立治理框架，绩效评价指标，能力标杆，貌似游离于安全之外，却是画龙点睛之笔。这是变“人治”为“法治”的关键！

“下君尽己之能，中君尽人之力，上君尽人之智”。

治理：是为了鼓励期望行为，而明确的决策权归属和责任担当框架。简而言之，就是明确权责，建立绩效标杆，让组织中的成员自觉drive自己对应的process，治理结构完善后方可成为“清静无为”的上君。

这还不完，任何法治都存在“不合理”“不近人情”之处，任何体系都需要不断的PDCA以日趋完善，所以有些地方还是需要变通的，变通不是为了耍小聪明，不是以身试法，而是为了弥补我们工作中的纰漏。

这一段可能比较深奥，其实这篇文章原来没这么长，也没有例如，是应了某人的要求而增加了不少解释性的内容。关于法治的问题，可以理解为国家的法律，地方的法律，在名为公司的企业组织内就表现为一系列西方管理学所推崇的制度、流程等。在流行的安全标准中，

Cobit是最贴近该领域的一个，想要quickstart可以借鉴一下这个，若要抓本质，就要去学“儒道法”。

10.技术体系

技术重要么？非常重要。否则就流于形式。但这并不是你要考虑的首要问题,招聘一名合适的技术经理是非常现实的问题。从管理的维度看，任何技术都只是最后的实现手段，问题只在于select哪一种。当试图解决问题时，应首先从管理的角度去分析，因为技术现象背后的本质往往是管理的问题。在执行的时候应恢复到具体的技术视角，这样不断的切换视角，变换维度才能在组织中、工作中的各个层面游刃有余。

技术对于CSO而言其实是一个可管理的过程，首先是要选择做“对的”事情，然后才是把事情做好。并不是什么事情都要做，有些事情看起来是“对的”，但在特定的阶段就不应该去做。有些事情，收效甚微，却执行繁琐，徒增加矛盾，吃力不讨好，那样的事情就不要做。安全建设应该Follow企业的“现状”，切不可一马当先。

另外一些事情可以让其他部门做，自己“后台管理”就行了，关键在于时刻明白自己在过程中所充当的“角色”。

之余，在技术的执行层面，标准流程，通用模型，做事方式都是比较重要的。

商业世界里不存在所谓的“真空”环境，CSO决不可能只是让你单纯的发布策略，写流程，写标准难么简单，那样的话人人都能当CSO了。

其实，信息安全管理最大的技能并不在于安全本身，如果你深切的理解“CSO不只是CSO”这句话时，你将发现你已经没有“上限”。

文中所述内容在于引导，不适用于“刻舟求剑”或“守株待兔”，因为每个人所处的“环境”不一样，但知“音”者皆能自渡。

-EOF-