怎样建立雅昌信息安全体系?

05

刘向东

近几年来，在集团高层的指导和支持下，公司在信息化建设和应用方面迈上了一个新台阶。不断提升和完善的信息化应用和服务，为公司日常办公、业务运营提供了便利和支持。然而，信息化是一把双刃剑，在给我们带来信息交换和获取的便捷的同时，也给信息安全埋下了隐患，如果不对其加以管控，后果将难以想象。

在商业竞争日益激烈的今天，一些组织和个人为了商业利益而无恶不作，黑客离我们已不再遥远，商业间谍也不再是传说。为避免我们辛辛苦苦拼来的商业秘密落入他人之手，我们必须主动加强对重要信息资产的保护，在信息自由流动的全过程进行安全监控和风险管理，将信息安全威胁和风险降至公司可控制和承受的程度。

为了保障公司的信息安全，我们必须建立一套有效的完整的统一的信息安全管理体系。依照ISO/IEC27001的内容，信息安全管理体系应当包括信息安全组织、信息安全策略、信息安全技术和信息安全运行等几个维度。不断变化的外部环境和日新月异的新技术，使得信息安全保护变得越来越困难。因此，唯有通过建立多位一体的信息安全管理体系，才能保障信息安全。

我们现在面临的主要问题是：

信息安全组织：尚未成立权威、独立的信息安全组织，致使信息安全工作无法推动、难以落实。缺乏信息安全专业人才。

信息安全策略：缺乏完整、清晰、统一的信息安全策略，虽有一些规范、流程和制度，但是还不完备、也未形成体系，执行缺位。

信息安全技术：虽然已采用多种信息安全技术对信息安全提供了基本保护，但是尚存在诸多不足，需要进一步完善。

信息安全运行：日常的安全运行多处于被动防御状态，缺乏明确的检查和处罚机制；缺乏应急响应机制和措施，对已有的安全设备的维护、升级和管理不到位。

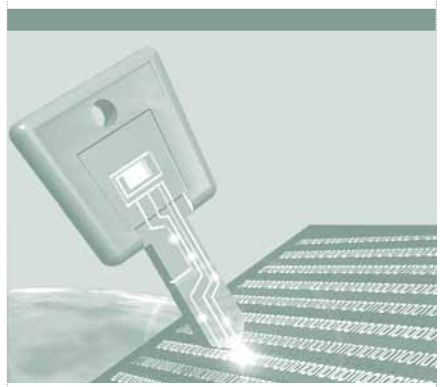
面对以上种种问题，我们必须认真思考以下问题：如何建立起有效的信息安全体系？信息安全组织该如何建立？信息安全技术是否有效可靠？信息安全运行是否有完整的制度保障？要解决这些问题，我们需要运用成熟的信息安全理论成果，借鉴敏感行业（比如高科技，金融等）的成功实践，设计出一套切合实际并融合策略、管理和技术于一体的信息安全体系（如图1），保障公司信息安全。

信息安全组织体系

做好信息安全工作主要还是要靠管理。信息安全管理意味着要改变用户的一些习惯和行为，这往往会招致用户不满和抵触，从而阻碍信息安全的推动和落实。倘若不能克服这个问题，要建立一套行之有效的信息安全体系几无可能。因此，建立和推行信息安全体系，需要一个强有力的信息安全组织来统筹和管理信息安全工作。公司应组建包括信息中心、法务、人力资源、行政及财务等部门共同参与的信息安全委员会。信息安全委员会要厘清信息安全各主体的角色及职责，对信息安全职责进行划分和约束，以尽力防止对关键流程的破坏。应加强信息安全的教育训练，提高全员的信息安全意识和认知水平，进而提升企业信息安全整体水平。要加大信息安全的宣贯，努力营造信息安全文化，将信息安全渗透到日常工作中，形成“信息安全，人人有责”的良好氛围。

信息安全策略体系

信息安全策略既包括管理层对信息安全的要求和指示，也包括各种规范、标准、制度、流程等。管理层对信息安全的要求和指示是信息安全工作的指导思想和行动方针。规范和标准是行业组织或厂商对信息安全制定的通用指南，供相关人员参考。制度是全员必须遵守的行为准则，明确了那些事情可以做那些事情不可做，并制定相应的奖惩措施，确保信息安全各项措施落到实处。流程是为避免操作人员配置和更改系统或网络设置不当而导致破坏网络及系统稳定的防范机制。信息安全策略应成为公司整体策略的一部分，必须高度重视和认真对待。



信息安全技术体系

目前普遍应用的信息安全技术有身份验证、访问控制、数字加密与签名、入侵检测/防御系统、VPN、防病毒/反间谍软件、存储备份与灾难恢复、漏洞扫描及审计追踪等，涵盖了信息安全的方方面面，也已广泛应用于各种安全产品和系统中。充分利用已成熟的理论和技术，结合公司自身的情况，选择合适的产品和技术来构建我们自己的信息安全技术体系无疑是一项十分有利且重要的工作。我们需要从以下几个方面着力：

物理安全：应当按照国标A或B类机房对中心机房的要求进行机房选址、装修和布置，配备冗余的电力、环境等支持设施，应强化防雷、防水、防火、防静电和防盗窃措施，应安

05

01>

图5> 信息安全组织体系

装门禁系统和高清监控系统；

网络安全：应建立高可用的网络基础设施；应采用VPN技术保护在公网上传送的私有数据；应采用AAA认证技术限制和记录登录和修改网络设备行为；应根据不同的安全级别对网络进行安全区域划分，在网络边界部署网络安全网关，在防火墙上设立DMZ区，将对公服务的系统放入，阻止外来用户进入内部网络，对内部网络形成缓冲，减少或避免病毒、木马和网络攻击对内部网络的直接冲击。

系统安全：系统安全主要是指操作系统和数据库系统的安全。要使用身份验证和访问控制技术对网络用户进行准入控制和授权管理，防止非法人员进入系统搞破坏和合法用户的不适当访问；要定期检查系统是否有安全漏洞，如有发现，应立即进行修补，防止零日攻击；要启用系统防火墙，关闭不必要的端口和网络服务；要加强对日志记录的审核和分析，监测系统异动行为，对日志审计的结果要存档，并予以保护。

数据安全：应保证数据在采集、处理、存储和传输过程中的安全，确保数据的完整性不被破坏、信息不被泄露、可用性不被降低。在数据处理之前，要对原始数据进行备份；在公网上传输数据，应使用VPN技术对数据进行适当的保护。

应用系统安全：开发应用系统前，应建立信息安全管控措施，识别系统开发周期中的信息安全弱点，把信息安全管理贯穿于开发的全过程，确保在应用系统开发的各个环节的信息

安全。开发完成后，还要对系统进行整体安全测试，只有完全符合相关安全要求后，方可投入使用。从外部引进的应用系统，要进行严格的信息安全检查和验收。

桌面安全：设置严格的有区别的系统策略，启用Windows系统防火墙；应及时修补系统及应用软件漏洞；要安装杀毒软件和安全卫士，定期对木马、病毒等恶意程序进行查杀；对USB接口进行管制；对浏览器Internet安全区域设置要严格。

无线网络安全：应建立统一SSID和身份验证的无线网络，只有授权用户才可进入无线网络。应对无线网络设备的登录进行身份识别和验证，严格授权和记录日志。

移动终端安全：移动设备包括但不限于以下电子设备：笔记本电脑，移动硬盘，U盘，MP3/MP4，IPAD，智能手机等。以上设备都能存取数据，可以通过USB接口或无线网络与公司信息系统直接交互，这会给信息安全造成严重威胁。随着公司移动终端越来越多，管理难度日益加大，信息安全威胁和风险不断增加，对移动终端进行安全管控已迫在眉睫，要建立一套严格的网络准入机制，启用身份识别和验证，实施访问控制措施，保全访问日志记录。

数据备份与恢复：要对重要数据进行保护，建立定期备份重要数据的机制，要保护好存有备份数据的存储介质，应避免将已备份存储介质与备份源存储介质放在同一个地方，防止因意外因素导致所有数据丢失。要建立应急恢复的机制，平时要进行应急恢复的演练，要熟练掌握数据恢复的技巧和操作流程，防止误操作，缩短系统恢复的时间，提高业务连续性。

信息安全运行体系：

信息安全运行就是要把信息安全体系落到实处，是整个信息安全体系中最重要的一环，直接关系到信息安全政策和制度能否得到执行并发挥预期的作用。因此要特别重视信息安全运行体系的建设，在部署之前，应根据行业普遍采用的PDCA戴明环（如图2）方法做好缜密计划，再依计划进行部署，要反复地检查是否存在漏洞和不足，对发现的问题要及时处理，持续改进。

02>

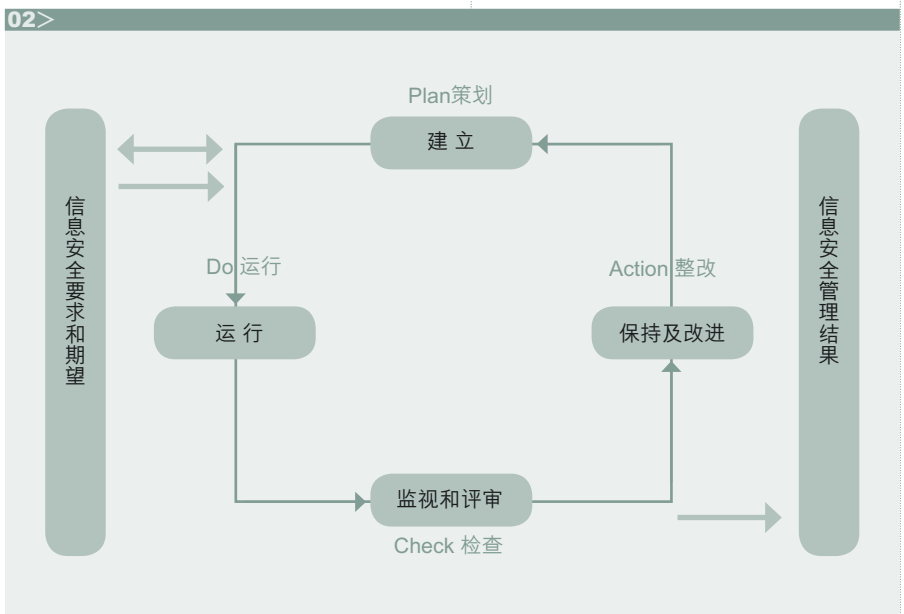


图2> 信息安全运行体系

随着雅昌发展战略的逐步落实，公司将产生一大批具体自主知识产权的技术、工艺和创意。正是这些技术、工艺和创意构成了雅昌的核心竞争力，让雅昌在未来激烈的商业竞争中永葆基业长青。因此，建立一套完整的有效的系统化的信息安全体系来保护公司的重要信息资产已势在必行。面对日益严峻的信息安全形势，为延缓、减轻或避免由此给公司造成的冲击和损失，我们有必要尽早尽快部署和推动信息安全工作，建立起一套实用管用可行的信息安全体系为公司的发展保驾护航。