《网络安全法》正式实施，这五个方面安全工作应尽快提上日程

（来源： 踏实实验室（WX：TS-SecLab）,2017-06-01）

今天,我国首部《网络安全法》正式实施。《网络安全法》的颁布与实施，不但从国家层面统一了对网络安全的认识，也使我国网络安全工作有了基础性法律框架。

根据国家相关立法要求，法律规定明确要求有关国家机关对专门事项作出配套的具体规定的，有关国家机关应当自法律施行之日起一年内作出规定。目前有关部门正在按照《网络安全法》的要求，抓紧制定相关配套规定，在未来一年内将会陆续颁布实施。

毫不夸张的说，从 2017 年开始国内所有企业、机构，尤其是与重要信息系统、重要公共服务、重要基础设施有关的单位，所面临网络安全压力将会越来越大。未雨绸缪方能从容应对，建议相关企业、机构等抓紧做好法律实施的准备工作，自觉用法律规范网络行为。

下面笔者就针对《网络安全法》实施后，相关企业、机构需要尽快提上日程的重点工作进行逐一分析。

一、等级保护制度是根本，网络安全等级保护需要从 1.0 升级到 2.0

《网络安全法》第 21 条明确规定了“国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第 31 条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

等级保护制度已经上升为法律，并在法律层面确立了其在网络安全领域的基础、核心地位。由此可见，网络安全等级保护制度依然是我国安全工作的根本制度，网络安全等级保护从 1.0 到 2.0 需要升级那些内容呢？

首先，等级保护 2.0 需要对保护对象进行扩展。等级保护 2.0 对保护对象进行扩展，不再只将信息系统作为保护对象，大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等均作为等级保护对象。

其次，等级保护 2.0 需要对保护内容进行完善。等级保护 2.0 将在定级、备案、建设整改、等级测评和监督检查五个规定动作的基础上，对等级保护的内涵进行丰富和完善。风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

最后，等级保护 2.0 需要对安全体系进行升级。等级保护 2.0 将建立更为完善的等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等内容。并围绕等级保护这个核心，构建起安全监测、通报预警、快速处置、态势感知、安全防范、精确打击等为一体的国家关键信息基础设施安全保卫体系。

二、监管检查压力持续增大，加快进行安全内控、合规体系建设

目前，作为我国网络安全“基本法”的《网络安全法》已经开始实施，继网络强国战略被纳入“十三五”规划建议后，《刑法修正案（九）》中也增加了对网络安全的诸多规定。

同时，作为网络安全工作的依据和制度，我国有关网络安全立法的步伐还要加快，《互联网安全法》、《商用密码管理条例》、《未成年人网络保护条例》、《个人信息保护法》等多项法律、法规正在起草或修订。

在网络安全检查方面，我国已经在 2006 年开始执行网络安全风险评估制度，2008 年开始逐步在政府部门建立起了网络安全检查制

度，《网络安全法》则正式建立了整个关键信息基础设施领域的网络安全检查制度。

从上面分析可以看出，未来所有企业、机构的安全合规压力会进一步加大。作为各单位的网络安全负责人，应提前着手开始准备组织自身的安全内控、合规体系建设，以应对未来严峻的网络安全监管形势。

三、个人信息保护是重中之重，敏感信息保护体系建设迫在眉睫

当前广大民众深受垃圾信息、诈骗信息、个人信息泄露的困扰，公民个人信息的泄露、收集、转卖，已经形成了完整的黑色产业链。

在《网络安全法》中对数据安全和个人隐私保护进行了明确的说明，以法律条文的形式规定了网络产品服务提供者、运营者的责任，并且严厉打击出售贩卖个人信息的行为。关于数据安全与个人隐私相关的《个人信息保护法》专项法律在不久的将来也会颁布，以填补我国在此领域的法律空白。

随着数据安全与个人隐私保护的法律的健全，当敏感信息泄露时责任单位所面临的除了自身名誉、客户、资金的损失外，还可能面对数据泄露后所负的刑事责任和赔偿责任。与之相对应的是，现在大多数单位在数据安全与个人隐私保护方面的防护措施都不是很到位，敏感数据泄露的途径和潜在风险非常的多。为能够适应形势的发展，考虑自身的切身利益，在此方面应该尽早做如下应对：

1）全面、系统地评估自身的敏感信息泄露途径与风险场景，并以此为基础建立具有针对性的安全策略。

2）综合运用技术产品与管理流程制度措施，全方面地进行数据安全与个人隐私保护建设，不断的封堵敏感信息泄露途径。

3）加大数据安全与个人隐私保护宣传教育，不断提升全体人员敏感信息保护意识，促进敏感信息保护文化建设。

四、关键信息基础设施应重点保障，新兴安全威胁需要重点防御

《网络安全法》中明确规定“可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网上安全等级保护制度的基础上，实施重点保护”，关键信息基础设施是我国网络安全保护的重点。

保障基础设施网络安全必然要实施具体的控制措施，在《网络安全法》多处条文都对具体的网络安全控制措施提出了明确要求。在这些条文中，不但对安全管理制度规范、防范计算机病毒与网络攻击入侵、数据备份与加密、安全机构、关键岗位人员、系统容灾、应急管理等等方面都提出了要求，对于网络日志的存储更是制定了需要至少保存六个月的详细规范。

在传统安全防护的基础上，网络安全将从被动防护转向积极防御进行转变，增强网络安全防御能力和震慑能力将是重中之重。那么，加强关键信息基础设施积极防御能力建设，需要从哪些方面着手呢？

首先，加大网络安全专业人才的培养与引进，建设能够具备网络安全对抗能力的队伍。

其次，在做好传统安全防护的基础上，逐步加强在持续安全威胁防御、安全态势感知等高级防御领域的能力建设。

最后，全面分析自身业务与数据的安全需求，全面开展安全产品技术与安全治理管理的融合工作，建立立体的网络安全防御体系。

五、自主可控是核心竞争力，自主知识产权网络产品应大力推广

我国网络安全技术距发达国家有一定差距，核心技术受制于人已经成为我国网络安全的软肋。想要提升我国的网络安全保障能力，只能依靠强大的科技实力和自主创新能力。《网络安全法》颁布实施后，将会重点构建国家网络空间安全技术体系，加快核心领域拥有自主知识产权的技术与产品的研发，并进一步推进自主知识产权安全产品应用推广。

出于整体网络安全战略考虑，将来网络安全产品采购将开始呈现国产化趋势，核心设备、系统将会逐步进行安全自主可控产品替换。

在此种情况下，各单位在进行安全自主可控建设的过程中，将不得不提早考虑相应的风险应对措施，比如：

1）使用具有自主知识产权的国产产品，以免将来部署完再进行替换所造成的资源浪费。

2）进行网络产品安全性评估与审查，尽量在国家、行业出台的合格供应商库中选取。

3）对现有网络安全产品进行国产化产品替换，应评估采用充分措施应对替换过程中的安全风险和产品兼容性问题。

总结

《网络安全法》的公布和施行，不仅从法律上保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，而且还有利于信息技术的应用，有利于发挥互联网的巨大潜力。

同时，网络安全能力已经成为企业、机构最重要的核心竞争力之一，做好网络安全并将其价值发挥最大，企业、机构才能在残酷的竞争中脱颖而出、扬帆远航！