君合研究简讯

JUNHE

2017 年 7 月 5 日

电信与互联网法律热点问题

网络安全事件应急预案

已于 2017 年 6 月 1 日生效的《网络安全法》（以下简称“**《网安法》**”）作为我国网络安全维护的第一部框架性法规，仍有很多具体制度和配套法规在制定之中。《网安法》第 51 条规定，“国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息”。

2017 年 6 月 27 日，中央网络安全和信息化领导小组办公室（以下简称“**中央网信办**”）印发了《国家网络安全事件应急预案》（以下简称“**《应急预案》**”）。

随着信息化的发展，网络安全事件对国家安全、社会稳定、个人利益的影响日益严重，而病毒攻击[1]、个人信息泄露[2]等事件屡见不鲜。《应急预案》旨在制定一套从国家到单位的网络安全事件应对方案。

一、网络安全事件的定义

网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件，除信息内容安全事件另行制定专项预案外，其余类型的网络安全事件均适用《应急预案》。（*1.3 条*）

二、新设国家网络安全应急办公室

根据《应急预案》规定，中央网信办特设国家网络安全应急办公室（以下简称“**应急办**”），负责网络安全应急跨部门、跨地区协调工作和国家网络安全事件应急指挥部的事务性工作等。同时，中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

三、网络安全事件的预警和响应

根据重要网络和信息系统遭受的损失程度、国家秘密、重要敏感信息和关键数据的丢失、被窃取等情况，以及事件对国家安全、社会秩序、经济建设、公共利益的影响程度，网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

[1] http://finance.ifeng.com/a/20170515/15375064_0.shtml
[2] http://www.chinacourt.org/article/detail/2017/03/id/2576962.shtml

针对不同等级的网络安全事件及其预警，《应急预案》制定了不同的预警发布、预警响应、应急响应以及调查与评估等措施。

例如，面对特别重大网络安全事件，红色预警响应措施包括：（1）应急办组织预警响应工作，对事态发展跟踪研判，研究制定防范措施和应急工作方案等；（2）有关省（区、市）、部门网络安全事件应急指挥机构实行 24 小时值班，保持联络畅通，加强网络安全事件监测和事态发展信息搜集工作，组织开展应急处置或准备、风险评估和控制工作，将重要情况报应急办等；（3）国家网络安全应急技术支撑队伍进入待命状态等。

四、《应急预案》项下的企业义务

根据《网安法》第 25 条和第 34 条的要求，网络运营者（一般企业）应当制定网络安全事件应急预案，而关键信息基础设施的运营者不仅应制定网络安全事件应急预案，还需要定期进行演练。

根据《网安法》和《应急预案》的要求，企业应及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，对网络安全事件进行调查和评估，采取技术措施和其他必要补救措施，消除安全隐患，防止危害扩大。如初判为特别重大或重大网络安全事件的，应将重要情况报应急办。

针对以上法律要求，企业需要重新审核内部网络安全管理的合规安排，例如，是否已建立健全应急工作机制；是否已制定网络安全事件应急预案；是否定期组织员工培训，确保员工了解在发现网络安全事件时的操作；是否在企业内部公开网络应急工作负责人的联系方式，确保员工能够第一时间联系到相关负责人；以及是否结合本企业情况制定判断特别重大、重大网络安全事件的标准，是否制定向应急办报告的流程等。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com
周梦瑶　律　师　电话：86 10 8519 1755　邮箱地址：zhoumy@junhe.com